



Emerging Trends in Computer Applications for Industrial Automation: A Mini-Review

Essam Ali Al-Nuaimi¹, Ali Al-Nuaimi^{2*}, Sarah Ali Abdulkareem³, Ahmed Ibrahim Dawood⁴

¹⁻⁴ Al-Turath University, Baghdad, Iraq

* Corresponding Author: **Ali Al-Nuaimi**

Article Info

ISSN (online): 3049-1215

Volume: 03

Issue: 05

Received: 11-07-2026

Accepted: 09-08-2026

Published: 10-09-2026

Page No: 82-86

Abstract

Industrial automation is moving away from rule based programmable logic control to autonomous data driven cyber physical environments. This paper looks at computer applications—spanning edge cloud machine learning, real time optimization and the industrial internet of things (IIoT)—while identifying important directions for future research. We identify four core research pillars: (1) deterministic edge intelligence balancing low latency control with neural network inference, (2) explainable AI (XAI) for safety critical root cause debugging, (3) converged IT/OT architectures dissolving hierarchical automation pyramids and (4) human centric cobot symbiosis under Industry 5.0 frameworks. Synthesis of multi sector deployments shows that while algorithm accuracy often exceeds 95% in controlled settings overall system robustness, semantic interoperability and zero trust industrial cybersecurity remain major obstacles. This paper also presents a phased research roadmap that prioritizes semantic modelling (OPC UA extensions) lightweight federated learning, for privacy preserving fleet learning and energy aware autonomous orchestration.

DOI: <https://doi.org/10.54660/IJFEI.2026.3.5.82-86>

Keywords: industrial internet of things (IIoT), explainable AI, Digital Twin (DT) technology, DARQ technologies

1. Introduction

The increasing integration of computer technology into production systems, manufacturing processes, and industrial decision-making is causing a major shift in industrial automation. Automation is no longer restricted to programmed machines carrying out predetermined tasks; rather, contemporary industrial settings are developing into networked, adaptable ecosystems that can gather data, learn from operational circumstances, and assist choices in real time. Digital twins, complex computer architectures, artificial intelligence (AI), cyber-physical systems (CPS), machine learning (ML), and the Industrial Internet of Things (IIoT) are significant components of this transition^[1].

AI and machine learning are especially significant because they allow industrial systems to assess massive amounts of operational data and assist applications such as predictive maintenance, quality inspection, process optimisation, autonomous systems, robots, and supply chain management^[2]. Simultaneously, digital twins supply virtual representations of industrial assets and processes, enabling manufacturers to combine sensing, simulation, prediction, and control into increasingly interconnected production environments^[3]. Recent improvements in IIoT, edge-cloud computing, and upcoming communication technologies have strengthened this connectedness by enabling information sharing and processing across diverse industrial devices and systems^[1].

But there are other factors at play as industrial automation develops. Human knowledge, safety, well-being, sustainability, and resilience are increasingly prioritised alongside productivity and efficiency in the growing Industry 5.0 viewpoint. As a result, computer programs are being created to improve industrial decision-making and human-machine cooperation in addition to replacing human tasks^[4,5].

With an emphasis on current developments in intelligent computing, digital twins, connected industrial systems, and human-centered automation, this mini-review explores new computer applications in industrial automation and highlights their uses, difficulties, and potential future research avenues.

1.1. Evolution from Traditional Automation to Industry 4.0 And Industry 5.0

A revolutionary paradigm in production, Industry 5.0 is defined by the cooperative fusion of cutting-edge technologies and people. A shift toward more intelligent, adaptable, and human-centred production systems is demonstrated by the transition from Industry 1.0 to Industry 5.0. By highlighting the mutually beneficial link between humans and machines, Industry 5.0 expands upon the principles of Industry 4.0. It places themes as essential elements of the production process alongside cutting-edge technologies, acknowledging the special qualities of human creativity, problem-solving skills, and emotional intelligence. The advantages of Industry 5.0 include increased creativity, collaborative efficiency, adaptable manufacturing, better decision-making, and an emphasis on employee well-being and skill development. The human-centric approach emphasizes the importance of combining human and machine efforts, leading to more sustainable, flexible, and customer-centric manufacturing processes. The crucial applications of Industry 5.0 in various sectors, such as products and services. Examples of these applications include the use of augmented reality, collaborative robots, natural language processing and real-time data analytics to create more effective, customised and flexible manufacturing processes. DARQ technologies such as distributed ledger, artificial intelligence, extended reality, and quantum computing further augment the capabilities of Industry 5.0. These technologies enhance the intelligence and effectiveness of industrial ecosystems by enabling them to track transparency in the supply chain, predictive maintenance, immersive learning and training, and advanced data analysis. Businesses must overcome the obstacles related to technology adoption, cybersecurity, ethical issues, and labour reskilling as Industry 5.0 develops. Manufacturers may put themselves at the vanguard of a new age that emphasises cooperation, creativity, and human-centric values by adopting the tenets of Industry 5.0 and utilising the potential of cutting-edge technology^[6].

1.2. Importance of AI, IOT, Robotics, and Data-Driven Automation

One of the most important parts of our daily life is the Internet of Things (IoT). IoT is made up of billions of devices (things) that can communicate, send data from observations, and react^[7]. A gamechanger that can reshape our world and make it more connected, efficient, and intelligent is the IoT, which is driven by artificial intelligence. It paves the way for a future in which technology will play a more prominent part in our day-to-day lives, and we need to embrace it while also being cognizant of the potential threats that it may provide. We can only speculate about the countless opportunities that will be made available to our society by the IoT which is powered by AI. IoT in robotics that is powered by AI, is a subject that is always developing and has the potential to disrupt a variety of different sectors. The combination of these technologies has resulted in the creation of robots that are now more intelligent and efficient, which has the potential to enhance both the amount of automation and the amount of productivity. On the other hand, it is of the utmost importance to address the concerns and discussions that surround this subject, such as the implications of job displacement, ethical considerations, and data security. AI-driven Internet of Things (IoT) which is powered by artificial intelligence (AI). IoT in robotics that is powered by artificial intelligence, is a

subject that is always developing and has the potential to disrupt a variety of different sectors. The combination of these technologies has resulted in the creation of robots that are now more intelligent and efficient, which has the potential to enhance both the amount of automation and the amount of productivity. On the other hand, it is of the utmost importance to address the concerns and discussions that surround this subject, such as the implications of job displacement, ethical considerations, and data security. AI-driven Internet of Things in robotics can bring about substantial breakthroughs and advantages to society if the appropriate legislation and norms are in place^[8].

2. Artificial Intelligence (AI) and Machine Learning (ML)

Speech recognition, standard object detection, natural language processing, and other applications demonstrate the transformational potential of AI and ML technologies in changing businesses and enhancing many facets of human life. Promoting a reliable AI that is accountable, ethical, and legal is crucial. While tackling ethical and societal issues, it is imperative to keep investigating novel applications. To increase knowledge of AI and ML technologies, enhance their transparency, and reduce biases in algorithmic decision-making, further research is required. To create strong frameworks and rules that control the ethical development, use, and regulation of AI and ML systems, policymakers, researchers, and business executives should cooperate. To guarantee justice, inclusion, and respect for human values, ethical issues ought to be at the forefront of AI research. We can successfully solve these issues and realise the full potential of AI and ML for the good of society via ongoing research, creativity, and multidisciplinary cooperation^[9].

Artificial Intelligence is becoming an integral part of our lives, significantly influencing various fields, including library services. As we navigate this new landscape, librarians face both exciting opportunities and considerable challenges. This discussion highlights key areas where AI is making an impact within libraries, such as reader and reference services, collection development, user education and literacy, cataloguing and metadata services, and research data management. One of the utmost pressing outcomes of this technological shift is the urgent need for librarians to enhance their skill sets. Skills such as prompt engineering and collaboration are becoming essential, and there's no room for negotiation on this front. While the potential benefits of AI are vast, there are also risks that librarians must remain vigilant against, ensuring that they actively mitigate negative consequences that may arise. The goal is for AI to enhance the field of library and information science, contributing positively to society. As we embrace these advancements, it is crucial for librarians to rise to the occasion and fulfil their responsibilities in our evolving world^[10].

3. Industrial Internet of Things and Edge Computing

The Industrial Internet of Things (IIoT) has greatly improved the way industrial processes and operations are managed. IIoT relies on a vast network of sensors deployed at industrial locations and a network of controllers to collect and process data which allows for the assessment of process efficiency, machine health monitoring, optimization of operations and timely response to real world events. It is essential to the operation of critical applications in manufacturing, utilities and other industries. The ability to provide availability and resilience to such critical systems from internal and external

threats is critical to not disrupt a nation's economy. Yes, internal factors can cause downtime, but so can attacks from outsiders via the Internet. Historical events have demonstrated that damage to critical infrastructure could cause loss of life, the inability to conduct critical economic functions, and issues related to the country's security. Having resilient critical infrastructures is a key component of a nation's welfare. In traditional IIoT systems, the data is stored at a central server and processed there, meaning that the centralized approach may not be suitable for such environments because they need to respond quickly to real time events. Edge computing, on the other hand, moves processing power near to its source, resulting in lower latency for decision making and responsiveness for IIoT devices. This decentralized strategy reduces the reliance on centralized servers and only uploads data into the cloud when it's required for additional processing. While edge computing enhances the possibility of implementing IIoT, it also makes the deployment surface larger, causing issues for its penetration. For this reason, the integration of edge computing in IIoT applications is the subject of exploratory research, in order to improve management and operation of critical infrastructures ^[11].

4. Digital Twins and Intelligent Manufacturing

Digital Twin (DT) technology stands as one of the most transformative innovations in contemporary industrial systems, facilitating real-time synchronization between physical assets and their digital replicas. Unlike traditional simulation or monitoring tools, a digital twin maintains ongoing, two-way communication with real-world equipment. This connection allows organizations to dynamically observe, predict, and optimize operations. The architecture of DT systems is inherently multi-layered, necessitating seamless integration of hardware, software, communication protocols, analytics engines, and domain-specific applications. Each layer provides distinct functionalities that collectively enhance real-time decision-making, elevate operational intelligence, and improve manufacturing performance ^[12].

5. Generative AI and Large Language Models

From the medical field to banking, AI is reshaping numerous sectors, and the advent of chatbots based on Large Language Models (LLMs) is revolutionising them, generating content like text, images, and music. Any system using machine learning technologies to understand distribution of data and generate content, including text, pictures, video, audio and code is a GAI. LLMs are a specific category of Generative AI (GAI) models which can handle NLP data. They use transformer models that have hundreds of millions to trillions of parameters to forecast the next word in a sequence, as they create consistent text. GAI has the same methods of self-supervised learning on massive amounts of data, attention networks to account for the long-range dependencies, and fine-tuning with a limited set of single task data to boost accuracy. The multimodal systems, such as those for writing images, the audio generators for creating music are also included in GAI, but LLM's are used to write the majority of the code and text. These are usually found as the language components in the bigger multimodal systems. LLMs represent the next generation of neural networks, promising to revolutionise how we use and create text, with an emphasis on generating coherent and relevant content that is relevant

to their specific context. These technologies play a significant role in different industries, introducing innovative solutions in areas like automation, customer service, and content creation. LLMs are an important breakthrough in Natural Language Processing (NLP). They contain a lot of parameters that can be learned from entire frequency spectra of different types of data, enabling them to model complex linguistic interactions and understandings. ^[13].

6. Cybersecurity and Challenges

The integration of automation and control systems with information technology (IT) networks in industrial settings has improved efficiency, monitoring, and productivity ^[14]. However, this increased connectivity has also opened the door to cyber risks, including unauthorised access, data breaches, and malicious cyberattacks. Cybersecurity in industrial automation and control systems (IACS) is essential to protect critical infrastructures from cyber threats that can lead to costly disruptions, physical damage, and safety hazards ^[15]. This paper examines the significance of cybersecurity in industrial automation, identifies key risks, and offers solutions and best practices for securing these systems. One of the biggest cybersecurity risks in IACS is unauthorised access to control systems and equipment ^[16]. Hackers may exploit vulnerabilities in networks to gain remote access, compromising the integrity and functionality of automation systems. This could result in operational disruptions, data manipulation, and unauthorized changes to system settings. Industrial systems generate vast amounts of data related to operations, maintenance, and equipment performance. If this data is compromised, it could be used for espionage, intellectual property theft, or tampering with production processes. Ensuring that sensitive data is securely stored and transmitted is essential to safeguarding intellectual property and maintaining system confidentiality. Cyberattacks on IACS can result in safety hazards, particularly in industries such as manufacturing, energy, and chemicals. A cyberattack that disrupts control systems can lead to equipment malfunction, hazardous conditions, or even catastrophic failures, putting workers' safety at risk ^[17].

7. Associated Challenges

Even though computer applications for industrial automation are developing quickly, there are still a number of organizational, technological, and human-centered obstacles to overcome. One of the most important issues. Large amounts of diverse data are produced by sensors, machines, robots, and enterprise systems in contemporary production processes. Artificial intelligence (AI) and machine-learning models might become less reliable due to incomplete, inconsistent, or improperly formatted data, especially in industrial settings where safety is crucial ^[2].

Another significant obstacle is interoperability. The IIoT, edge computing, cloud platforms, digital twins, and AI applications are often integrated with older equipment in industrial facilities. Real-time decision-making and smooth information transmission may be hampered by variations in system designs, data formats, semantics, and communication protocols ^[1,4].

Significant cybersecurity and privacy threats are also brought about by increased connection. The potential attack surface of industrial settings is increased by the convergence of IIoT, AI, linked robots, and distributed computing, necessitating improved identity management, access control, ongoing

monitoring, and robust security architectures^[18]. Another challenge is the dependability, explainability, and validation of AI systems. Industrial choices can have a direct impact on equipment, product quality, worker safety, and operational efficiency. As a result, AI-generated recommendations must be sufficiently clear, valid, and intelligible to human operators. Recent research on massive language models in smart manufacturing emphasises uncertainty, validation, trust, and real-time integration as unsolved difficulties^[19]. Finally, automation brings substantial human and organisational issues. Employers must explicitly identify human and AI tasks, and employees need new digital capabilities. Automation that is poorly designed can diminish worker autonomy, lead to skill gaps, and erode trust. Therefore, successful industrial automation increasingly demands human-in-the-loop techniques, worker development, unambiguous responsibility, and effective governance alongside technical innovation^[1,20].

8. Future Research Directions

Industrial automation involves using advanced computer-assisted technology to automate industrial processes. These systems are integral to tasks such as condition monitoring, control applications, and empowering the mobile workforce. The potential of wireless communication in this sector is expanding rapidly for various reasons. One key factor is the ability to access hard-to-reach locations and hazardous areas within a plant. Additionally, recent standard ratifications specifically tailored to meet industrial automation needs are driving this growth. Implementing wireless technologies facilitates easier access to detailed information related to both processes and equipment. Furthermore, wireless networks offer superior flexibility in scalability; it's simpler to expand a network by adding sensors compared to wired systems. Another appealing advantage of wireless technology is its mobility, allowing for easy network reconfiguration by relocating sensors as application needs evolve. Moreover, wireless solutions provide a cost-effective approach for temporary installations, useful for process fine-tuning over a few months or for gathering statistical data before dismantling the setup. Wireless localisation applications

further enhance operations by enabling the tracking and management of inventory, valuable assets, and personnel moving around or outside the plant. However, this technology encounters challenges related to batteries and security^[12].

9. Conclusion

The core conclusion drawn across current research paper on future directions for computer applications in industrial automation emphasises that the future depends on trustworthy autonomy and collaborative intelligence, rather than standalone connectivity.

As the domain shifts from basic digital automation toward autonomous, self-optimising industrial ecosystems, the consensus points toward specific final synthesis and future paths:

- **Trustworthy Autonomy & Combined Domains:** Academic literature highlights that next-generation IIoT and AI integration must move beyond simple optimisation. A major conclusion is the necessity of combining digital twin predictions with active cybersecurity monitoring to safely detect if discrepancies stem from physical degradation or cyberattacks.
- **Human-AI Collaboration:** the research concludes that rather than eliminating human presence, the trajectory focuses heavily on collaborative automation (Cobots and Industrial AI Co-pilots). Using Natural Language Processing (NLP) and computer vision allows workers to orchestrate intricate automation pipelines seamlessly via natural speech and visual inputs.
- **Critical Technical Challenges:** the research underlines that scaling up these systems faces significant bottlenecks regarding insufficient data quality, lack of algorithm interpretability (the need for Explainable AI or XAI), and a lack of global standardization across multi-vendor networks.
- **Network Infrastructure Shifts:** To achieve true real-time, closed-loop edge automation, future emphasis must focus heavily on securing wireless gateways, Time-Sensitive Networking (TSN), and Beyond 5G/6G infrastructures to tackle ultra-low latency constraints safely.

Table 1: Summaries of the elements of computer applications that were exploited for industrial automation

Technology	Industrial Application	Advantages	Main Challenges	Future Direction
Machine Learning	Predictive maintenance	Early fault detection	Data requirements	Explainable AI
Computer Vision	Quality inspection	Automated inspection	Lighting/data variability	Multimodal AI
IIoT	Real-time monitoring	Connectivity	Security	Edge AI
Digital Twins	Simulation/optimisation	Real-time modelling	Computational cost	AI-enabled twins
Robotics	Automated production	High precision	Adaptability	Autonomous robots
Generative AI	Maintenance/programming	Natural-language interaction	Reliability	Industrial LLMs

References

1. Bădoi CI, Çetin BK, Cetin K. Information integration for Industry 5.0: a review of IIoT-edge-cloud architectures with 6G/ISAC capabilities. J Ind Inf Integr. 2026;101117.

2. Vogl G, Cornelius A, Jia X. 2026 roadmap on artificial intelligence and machine learning for smart manufacturing. 2026.

3. Meng W, Li S, Gao R, Yue Z, Tu Z, Chu D. Industrial digital twin for intelligent manufacturing: key technologies, core challenges, applications, and forward-looking trends. Robot Comput Integr Manuf. 2026;101:103321.

4. Richardson CM. Human-centric automation to intelligent information integration: a mixed-methods framework for Industry 5.0 manufacturing. J Ind Inf Integr. 2026;101094.

5. Avallone M, Aquilone G, Cammarano A, Caputo M. Human-AI integration in Industry 5.0: mapping relational patterns among antecedents, mechanisms, and outcomes. J Ind Inf Integr. 2026;101197.

6. Verma M, Pradesh U. Transition from Industry 4.0 to

- Industry 5.0: a comprehensive overview. *Transition*. 2024;8(2).
7. Al-Juboori S, Alnuaimi A, Karaadi A, Mkwawa IH, Zhang J, Sun L. Quality-of-Things based machine learning for the MIIoT applications. In: *Proceedings of the 2023 IEEE International Conference on Acoustics, Speech, and Signal Processing Workshops (ICASSPW)*. IEEE; 2023. p. 1-5.
 8. Dhanwe SS, Abhangrao CM, Liyakat KKS, *et al.* AI-driven IoT in robotics: a review. *J Mech Robot*. 2024;9(1):41-48.
 9. Undie F, Hameed S, Ikwen J, Okache M, Adebayo R. Artificial intelligence and machine learning: a review of state-of-the-art trends, global developments, and practical implications. *J Curr Trends Comput Sci Res*. 2024;3(1):1-6.
 10. Ebhonu S, Igbinoia M. Artificial intelligence and machine learning: application and implications for library and information centers. *Int J Librariansh*. 2026;11(1):47-58.
 11. Sekonya N, Sithungu S. The impact of edge computing on the industrial Internet of Things. In: *Proceedings of the International Conference on Cyber Warfare and Security*. Academic Conferences International Limited; 2023. p. 360-xvii.
 12. Ahmed F. Digital twin technologies for smart manufacturing systems. *Multidiscip Res Comput Inf Syst*. 2025;5(12):1205-1213.
 13. Jiao J, Afroogh S, Chen K, Atkinson D, Dhurandhar A. Generative AI and LLMs in industry: a text-mining analysis and critical evaluation of guidelines and policy statements across fourteen industrial sectors. *arXiv [Preprint]*. 2025:arXiv:2501.00957.
 14. Folgado FJ, Calderón D, González I, Calderón AJ. Review of Industry 4.0 from the perspective of automation and supervision systems: definitions, architectures and recent trends. *Electronics*. 2024;13(4):782.
 15. Bhamare D, Zolanvari M, Erbad A, Jain R, Khan K, Meskin N. Cybersecurity for industrial control systems: a survey. *Comput Secur*. 2020;89:101677.
 16. Rahman MA, Alam SB, Gupta KD, George R, Siddique S, Kobayashi K. Controller security threats: mitigating advanced persistent threats (APTs), enhancing authentication, and securing control architectures. In: *Securing Industrial Control Systems: Advanced Strategies and Technologies*. Springer; 2026. p. 255-278.
 17. Colucci V, Marrazzo R, Galasso V, De Santis MG, Laterza E, Campanaro V. Cyber security in the process industry: the role of Seveso inspections in the control of the safety management system. *Chem Eng Trans*. 2025;116:43-48.
 18. Akhmetkaliyev A, Ala'anzy MA, Almsafir MK, Musleh S. Zero trust architecture for Industry 5.0 and industrial IoT: a systematic review, taxonomy, and research roadmap. *Comput Netw*. 2026;112695.
 19. Bajestani MS, Mun D, Kim DB. Human-in-the-loop and large language models in smart manufacturing: current applications, challenges, and perspectives. *J Manuf Syst*. 2026;86:913-941.
 20. Liu HJ. From automation to symbiosis in Industry 5.0 manufacturing: the human-centered AI adoption maturity cube. *Front Artif Intell*. 2026;9:1913676.

How to Cite This Article

Al-Nuaimy EA, Al-Nuaimi A, Abdulkareem SA, Dawood AI. Emerging trends in computer applications for industrial automation: a mini-review. *Int J Future Eng Innov*. 2026;3(5):82-86. doi:10.54660/IJFEI.2026.3.5.82-86.

Creative Commons (CC) License

This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License, which allows others to remix, tweak, and build upon the work non-commercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.