

Autonomous Intelligent Systems for Future Digital Ecosystems

Prof. Diana Inkpen

Professor, University of Ottawa, Canada

Abstract

Autonomous intelligent systems are becoming an important foundation for future digital ecosystems because they can perceive information, analyze complex environments, make decisions, and perform actions with limited human intervention. The integration of artificial intelligence, machine learning, Internet of Things technologies, edge computing, cloud platforms, robotics, and intelligent communication networks has expanded the capabilities of autonomous systems across industrial, commercial, public, and social environments. This paper examines autonomous intelligent systems for future digital ecosystems through a conceptual and literature-based research approach. The study focuses on autonomous perception, intelligent decision-making, adaptive learning, distributed intelligence, interconnected devices, human-machine interaction, and digital infrastructure.

The analysis indicates that autonomous systems can improve operational responsiveness, resource utilization, automation, and decision support by continuously processing information from interconnected digital environments. However, challenges involving system reliability, cybersecurity, explainability, data governance, interoperability, computational resources, ethical responsibility, and human acceptance remain significant. The study emphasizes the importance of adaptive architectures, edge intelligence, secure communication, interoperable platforms, and responsible AI mechanisms for future autonomous digital environments.

Future research should investigate self-adaptive systems, collaborative autonomous agents, explainable decision-making, decentralized intelligence, digital twins, energy-efficient computing, and trustworthy autonomous operations. The study concludes that autonomous intelligent systems can contribute substantially to future digital ecosystems when technological autonomy is combined with reliability, security, transparency, interoperability, and human-centered governance.

Keywords: Autonomous Intelligent Systems, Digital Ecosystems, Artificial Intelligence, Machine Learning, Edge Computing, Internet of Things, Autonomous Agents, Intelligent Automation, Digital Transformation, Distributed Intelligence.

1. Introduction

Digital ecosystems have evolved from isolated computing environments into interconnected infrastructures in which devices, applications, organizations, users, platforms, and intelligent technologies continuously exchange information. The increasing availability of connected sensors, cloud platforms, edge computing, artificial intelligence, and advanced communication networks has created

opportunities for developing systems that can operate with greater autonomy. Autonomous intelligent systems represent an important development within this transformation because they can interpret information and perform decisions or actions with reduced direct human intervention.

Artificial intelligence provides the computational foundation for many autonomous systems. Machine learning enables systems to identify patterns from data, while intelligent agents can use environmental information to select actions according to defined objectives. The development of autonomous systems has therefore moved beyond conventional rule-based automation toward systems capable of adaptation and context-sensitive decision-making. These capabilities are particularly relevant to digital ecosystems characterized by large volumes of continuously generated and heterogeneous data.

Edge computing and Internet of Things technologies further strengthen autonomous digital environments. Connected sensors can generate information from physical and digital environments, while edge platforms can process selected information closer to its source. This distributed approach can reduce communication delays and support localized decision-making. Cloud infrastructure can provide additional computational resources for complex workloads, creating opportunities for hybrid architectures in which intelligence is distributed across devices, edge platforms, and centralized systems.

The expansion of autonomous intelligence also introduces important concerns. Digital ecosystems contain interconnected components that may have different security requirements, computational capabilities, communication standards, and operational objectives. An autonomous decision generated by one component can consequently affect other connected components. Reliability, cybersecurity, interoperability, explainability, privacy, accountability, and human oversight therefore become important considerations when autonomous systems operate within complex digital environments.

Autonomous intelligent systems require comprehensive development frameworks that integrate technological capability with responsible system design. This paper examines autonomous intelligent systems for future digital ecosystems through a conceptual and literature-based approach. It analyzes the technologies supporting autonomous intelligence, application areas, major challenges, and future research opportunities. The study emphasizes that future digital ecosystems should combine autonomy with security, adaptability, transparency, interoperability, and appropriate human involvement.

2. Objectives of the Study

2.1 Primary Objective

The primary objective of this study is to examine autonomous intelligent systems for future digital ecosystems and to evaluate how artificial intelligence, machine learning, edge computing, Internet of Things technologies, intelligent agents, distributed computing, and adaptive decision-making can support responsive, scalable, secure, and intelligent digital environments.

The study also seeks to identify the technological and organizational factors influencing autonomous system performance. Particular attention is given to adaptability, computational resources, communication, interoperability, cybersecurity, explainability, reliability, privacy, human oversight, and responsible governance as important conditions for sustainable autonomous digital ecosystems.

2.2 Examination of Autonomous Intelligence Technologies

The first objective is to examine the major technologies supporting autonomous intelligent systems, including artificial intelligence, machine learning, intelligent agents, IoT devices, edge computing, cloud computing, digital twins, distributed intelligence, and advanced communication networks. The study considers their contribution to autonomous perception and decision-making.

The objective further examines how these technologies can operate collectively within digital ecosystems. IoT devices provide continuous information, while edge and cloud platforms support computational processing. Intelligent agents can interpret available information and select appropriate actions. Their integration can enable adaptive and distributed digital environments with reduced dependence on continuous human intervention.

2.3 Assessment of Future Digital Ecosystem Applications

The second objective is to assess potential applications of autonomous intelligent systems across smart cities, industrial ecosystems, healthcare, transportation, smart buildings, financial services, agriculture, energy systems, and digital business environments. The study considers how autonomous capabilities can improve operational coordination and decision support.

The objective also examines factors influencing successful adoption, including system reliability, cybersecurity, interoperability, data governance, scalability, computational efficiency, and human acceptance. Future digital ecosystems should therefore balance autonomous operation with appropriate oversight and governance mechanisms. The study seeks to identify an integrated perspective for developing trustworthy autonomous digital environments.

3. Review of Literature

3.1 Autonomous Intelligent Systems and Intelligent Agents

Autonomous intelligent systems are closely associated with intelligent agents capable of perceiving environments and selecting actions according to objectives. Wooldridge describes intelligent agents as computational systems that operate autonomously within environments and can exhibit goal-directed behavior. This concept provides a theoretical foundation for autonomous systems operating within complex digital environments.

Recent developments in artificial intelligence have expanded autonomous capabilities through machine learning, deep learning, reinforcement learning, and knowledge-based reasoning. Autonomous systems can increasingly process heterogeneous information and adapt their behavior according to changing conditions. However, autonomy also creates requirements for reliable decision-making, appropriate constraints, monitoring, and validation, particularly when systems operate in interconnected environments.

3.2 IoT, Edge Computing, and Distributed Intelligence

The Internet of Things provides a major infrastructure for future digital ecosystems by connecting physical devices, sensors, and computational systems. Gubbi et al. describe IoT as an interconnected environment involving sensing, communication, computation, and intelligent services. Such connectivity enables digital ecosystems to continuously collect information from physical environments.

Edge computing extends this architecture by moving computation closer to data sources. Shi et al. explain that edge computing can address latency and bandwidth challenges by placing computational resources near end devices. The combination of IoT and edge intelligence can therefore support localized autonomous decision-making, while cloud infrastructure can provide additional resources for computationally intensive operations.

3.3 Digital Ecosystems and Adaptive Computing

Digital ecosystems involve interactions among heterogeneous technological and organizational components. Digital ecosystem research emphasizes distributed participation, connectivity, adaptation, and interactions among multiple actors. Autonomous intelligent systems can strengthen these environments by dynamically responding to changing information and operational requirements.

Adaptive computing further supports autonomous behavior by allowing systems to modify processes according to environmental conditions. Digital twins, machine learning, and intelligent orchestration can support monitoring and optimization within complex digital environments. Future ecosystems are therefore likely to combine distributed intelligence with adaptive infrastructure, enabling systems to coordinate activities while maintaining appropriate security and governance controls.

4. Research Methodology

4.1 Research Design

This study adopts a conceptual and literature-based research design to examine autonomous intelligent systems for future digital ecosystems. The research focuses on artificial intelligence, machine learning, intelligent agents, Internet of Things technologies, edge computing, cloud infrastructure, distributed intelligence, digital twins, and autonomous decision-making. The conceptual approach supports systematic examination of technological relationships.

The study does not introduce fabricated experimental observations, survey results, or unsupported numerical performance claims. Instead, academic literature addressing autonomous systems, intelligent agents, IoT, edge computing, AI, and digital ecosystems is reviewed thematically. This approach enables identification of recurring technological capabilities, application patterns, implementation challenges, and future research directions associated with autonomous digital environments.

4.2 Literature Collection and Organization

The literature was organized according to major technological dimensions, including autonomous intelligence, sensing, machine learning, intelligent agents, edge computing, cloud systems, communication, and digital ecosystem integration. Studies were considered relevant when they addressed autonomous decision-making, distributed intelligence, connected digital environments, or intelligent system adaptation.

The literature was further categorized according to application areas including smart cities, industrial systems, healthcare, transportation, energy, agriculture, smart buildings, and digital business environments. Recurring themes such as autonomy, adaptability, interoperability, cybersecurity, privacy,

explainability, scalability, reliability, and human oversight were identified to establish a structured foundation for analysis.

4.3 Analytical Framework

The analytical framework evaluates autonomous intelligent systems through five dimensions: perception, intelligence, decision-making, action, and ecosystem integration. Perception concerns the collection of environmental information through sensors and digital data sources. Intelligence involves AI and machine learning capabilities. Decision-making addresses selection of appropriate responses according to objectives.

Action represents automated execution through software or connected physical devices. Ecosystem integration concerns communication and coordination among devices, platforms, users, and organizations. Cross-cutting factors including security, reliability, privacy, interoperability, explainability, energy efficiency, and governance are also considered within the analytical framework.

4.4 Data Analysis Approach

A thematic analysis approach was used to examine recurring patterns across the reviewed literature. Technological capabilities, application benefits, operational limitations, and emerging research directions were compared across different autonomous system environments. The analysis focuses on relationships between autonomous intelligence, distributed computing, connectivity, and digital ecosystem performance.

The identified themes were subsequently organized into technology, application, and challenge categories. This organization supports systematic comparison of autonomous intelligent systems across different digital environments. The approach provides a conceptual foundation for understanding how autonomy can be integrated with interconnected infrastructures while maintaining reliability, security, interoperability, and appropriate human oversight.

5. Analysis

5.1 Technologies Supporting Autonomous Digital Ecosystems

Autonomous digital ecosystems depend on multiple technologies that collectively enable systems to sense, analyze, communicate, decide, and act. Artificial intelligence provides computational intelligence, while IoT technologies provide continuous information from connected environments.

Edge and cloud computing offer complementary processing capabilities, and communication technologies connect distributed components. summarizes the principal technologies supporting autonomous intelligent systems.

Table 1: Core Technologies Supporting Autonomous Intelligent Systems

Technology	Primary Function	Contribution to Autonomy
Artificial Intelligence	Intelligent analysis	Autonomous reasoning
Machine Learning	Pattern learning	Adaptive behavior
Intelligent Agents	Goal-oriented operation	Autonomous decision-making
Internet of Things	Connected sensing	Environmental awareness
Edge Computing	Local processing	Low-latency intelligence
Cloud Computing	Large-scale computation	Complex analytics
Digital Twins	Virtual representation	Monitoring and optimization
Communication Networks	Data exchange	System coordination
Knowledge Systems	Information representation	Context-aware reasoning
Automation Platforms	Task execution	Reduced human intervention

Interpretation: demonstrates that autonomous intelligent systems rely on complementary technologies rather than a single computational mechanism. Artificial intelligence and machine learning provide analytical and adaptive capabilities, while intelligent agents support goal-oriented decision-making. IoT technologies supply information from connected environments.

Edge computing supports local processing, whereas cloud computing can provide greater computational capacity. Digital twins support virtual monitoring and optimization. Communication networks enable coordination among distributed components, while knowledge systems provide contextual information. Automation platforms translate decisions into operational actions, collectively supporting autonomous digital ecosystem functionality.

5.2 Applications of Autonomous Intelligent Systems

Autonomous intelligent systems can support digital environments where continuous monitoring, adaptive decision-making, and automated coordination are required. Their applications extend across physical infrastructure, business processes, public services, and connected environments. presents major application areas and the potential contribution of autonomous intelligence.

Table 2: Applications of Autonomous Intelligent Systems

Application Area	Autonomous Function	Potential Contribution
Smart Cities	Intelligent infrastructure coordination	Responsive urban services
Smart Manufacturing	Autonomous process optimization	Production efficiency
Healthcare	Intelligent monitoring	Decision support
Transportation	Autonomous traffic management	Mobility optimization
Smart Buildings	Automated environmental control	Resource efficiency
Agriculture	Intelligent field monitoring	Precision management
Energy Systems	Demand and resource optimization	Efficient energy management
Logistics	Autonomous routing	Operational coordination
Financial Services	Automated analytics	Decision support
Digital Business	Workflow automation	Process efficiency

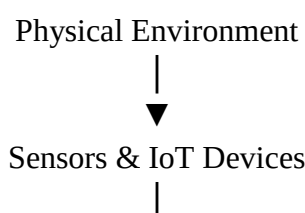
Interpretation: illustrates the wide application potential of autonomous intelligent systems. Smart cities can use autonomous intelligence for infrastructure coordination, while manufacturing environments can apply intelligent systems to optimize processes. Healthcare applications can support monitoring and decision-making, whereas transportation systems can use autonomous technologies for traffic management.

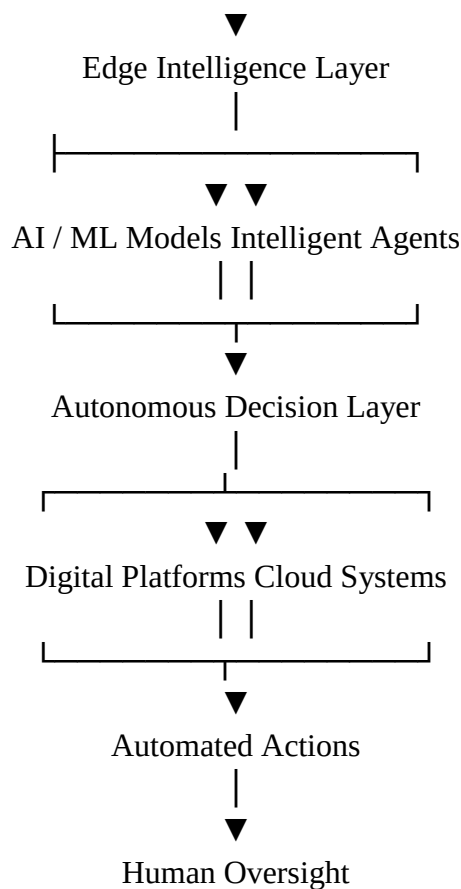
Smart buildings can automate environmental controls, while agriculture can use intelligent monitoring. Energy systems can benefit from resource optimization, and logistics can employ autonomous routing. Across these sectors, autonomous intelligence can improve responsiveness and coordination while reducing repetitive human intervention.

5.3 Autonomous Digital Ecosystem Architecture

Future digital ecosystems require an architecture capable of connecting physical devices, edge systems, cloud platforms, intelligent agents, and human users. The architecture should allow information to move across different layers while enabling autonomous decision-making close to the source when required.

Figure 1: Conceptual Architecture of an Autonomous Digital Ecosystem





Interpretation: The architecture illustrates a distributed approach to autonomous digital ecosystems. Sensors and IoT devices collect information from the physical environment, while edge intelligence enables local processing. AI models and intelligent agents analyze information and contribute to autonomous decision-making. Cloud systems and digital platforms provide additional computational and coordination capabilities.

Automated actions can then be executed through connected systems. Human oversight remains an important component, particularly for high-impact decisions. The architecture therefore combines technological autonomy with layered processing, connectivity, monitoring, and appropriate human involvement.

6. Discussion

Autonomous intelligent systems can significantly influence the development of future digital ecosystems by enabling continuous perception, analysis, decision-making, and action. Unlike conventional automation, which generally follows predefined procedures, autonomous systems can use information from their environment to adjust their behavior. This capability is particularly relevant to dynamic digital environments where conditions, data patterns, and operational requirements can change continuously.

The integration of IoT, edge computing, and artificial intelligence creates opportunities for distributed autonomy. IoT devices can provide continuous environmental information, while edge systems can process time-sensitive information close to its source. Cloud infrastructure can support more

computationally demanding operations. This layered architecture can reduce dependence on centralized processing while allowing intelligent capabilities to be distributed across multiple digital ecosystem components.

However, increased autonomy also creates new requirements for security, reliability, transparency, and governance. An autonomous system operating within a connected ecosystem may influence other systems through automated decisions. Errors can therefore propagate across interconnected components. Future digital ecosystems should incorporate monitoring, access control, explainability, human oversight, fault detection, and responsible governance. Autonomy should consequently be treated as a system-level capability requiring continuous evaluation rather than simply as an AI feature.

7. Challenges

7.1 System Complexity and Interoperability

Future digital ecosystems contain heterogeneous devices, software platforms, communication protocols, and computational infrastructures. Integrating these components into autonomous systems can create significant technical complexity. Different devices may use incompatible standards or data formats, limiting seamless communication and coordinated decision-making.

Interoperability is particularly important when autonomous systems operate across organizational and technological boundaries. A decision generated by one system may require information from another platform or device. Standardized interfaces, common communication protocols, modular architectures, and interoperable data formats can improve coordination. Future autonomous ecosystem frameworks should therefore address interoperability from the initial architecture stage rather than attempting to resolve compatibility issues after deployment.

7.2 Reliability and Autonomous Decision-Making

Autonomous systems must produce appropriate decisions under changing and sometimes uncertain conditions. Machine learning models can generate incorrect outputs when exposed to unfamiliar data or environmental conditions. Such errors can become more significant when automated decisions influence connected systems or physical operations.

Reliability therefore requires continuous monitoring, validation, testing, and fault-detection mechanisms. Systems should also include appropriate fallback procedures when confidence is low or abnormal conditions are detected. Human oversight may remain necessary for high-impact applications. Future research should develop autonomous architectures that combine adaptive intelligence with predictable behavior, transparent decision processes, and mechanisms for detecting and managing uncertainty.

7.3 Cybersecurity and Data Governance

Interconnected digital ecosystems increase the number of potential entry points for cyber threats. Autonomous devices, communication networks, edge systems, and cloud platforms can each introduce vulnerabilities. A security compromise could potentially affect automated decisions or disrupt interconnected services.

Data governance is equally important because autonomous systems depend heavily on continuous data collection and processing.

Information may include operational, environmental, or user-related data. Secure authentication, encryption, access control, privacy-preserving methods, continuous security monitoring, and responsible data-management practices are therefore essential. Future autonomous ecosystem frameworks should incorporate cybersecurity and data governance throughout the complete system lifecycle.

7.4 Explainability, Human Acceptance, and Governance

Autonomous decision-making can create difficulties when users cannot understand why a system produced a particular decision. Lack of transparency may reduce trust, especially in applications involving healthcare, finance, public services, or critical infrastructure. Explainable AI can help communicate relevant decision factors, although explanations must remain understandable and appropriate to the application.

Human acceptance also depends on perceptions of safety, usefulness, fairness, and control. Excessive autonomy may create concerns about accountability and responsibility when decisions produce undesirable outcomes. Governance frameworks should therefore define appropriate levels of human involvement, system responsibility, monitoring, and intervention. Future digital ecosystems should balance autonomy with meaningful human oversight.

8. Future Research

Future research should investigate self-adaptive autonomous systems capable of adjusting computational resources, decision strategies, and operational behavior according to changing environmental conditions. Research should also examine collaborative autonomous agents that can coordinate tasks across distributed digital ecosystems while maintaining system-level objectives, security, and reliability.

Further research should explore explainable autonomous decision-making, decentralized intelligence, digital twins, and edge-cloud cooperation. Distributed AI could enable local decision-making while cloud systems provide additional analytical capabilities. Digital twins can support simulation and continuous monitoring of autonomous ecosystems. These technologies could strengthen system adaptability while providing additional mechanisms for testing and optimization.

Future empirical research should evaluate autonomous systems using standardized measures covering decision accuracy, response latency, reliability, resource utilization, energy consumption, cybersecurity, interoperability, explainability, and human acceptance. Comparative studies across smart cities, manufacturing, healthcare, transportation, agriculture, and energy environments could identify application-specific requirements and support the development of more trustworthy and scalable autonomous digital ecosystem architectures.

9. Conclusion

Autonomous intelligent systems represent an important technological direction for future digital ecosystems because they enable interconnected environments to perceive information, analyze conditions, make decisions, and execute actions with reduced human intervention. Artificial intelligence,

machine learning, IoT, edge computing, cloud platforms, intelligent agents, and digital twins provide complementary capabilities that can support increasingly adaptive and responsive digital infrastructures.

The analysis demonstrates that autonomy is a system-level capability dependent on multiple technological components. Sensors and IoT devices provide environmental information, while edge and cloud systems provide computational resources. AI models and intelligent agents support analysis and decision-making, and automation platforms execute resulting actions. Effective integration among these components is necessary for achieving reliable autonomous behavior across diverse digital environments.

Several challenges continue to influence the development of autonomous digital ecosystems. System complexity, interoperability, reliability, cybersecurity, data governance, explainability, human acceptance, and accountability require careful attention. Autonomous decisions can affect interconnected systems, making monitoring and validation essential. Appropriate human oversight is therefore particularly important for applications involving significant operational, social, or economic consequences.

Overall, autonomous intelligent systems can provide a strong foundation for future digital ecosystems when autonomy is developed alongside security, transparency, interoperability, reliability, and responsible governance. Future research should emphasize self-adaptive systems, distributed intelligence, collaborative agents, explainable AI, edge-cloud architectures, and digital twins. A balanced approach can support digital ecosystems that are more intelligent, responsive, scalable, secure, and capable of adapting to future technological requirements.

References

1. Albrecht, S. V., & Stone, P. (2018). Autonomous agents modelling other agents: A comprehensive survey and open problems. *Artificial Intelligence*, 258, 66–95. <https://doi.org/10.1016/j.artint.2018.01.002>
2. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50–58. <https://doi.org/10.1145/1721654.1721672>
3. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. <https://doi.org/10.1016/j.comnet.2010.05.010>
4. Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications*, 19, 171–209. <https://doi.org/10.1007/s11036-013-0489-0>
5. Colakovic, A., & Hadzialic, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks*, 144, 17–39. <https://doi.org/10.1016/j.comnet.2018.07.017>
6. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
7. Jennings, N. R., Moreau, L., Nicholson, D., Ramchurn, S., Roberts, S., Rodden, T., & Rogers, A. (2014). Human-agent collectives. *Communications of the ACM*, 57(12), 80–88. <https://doi.org/10.1145/2621935>

8. Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, 79, 1–14. <https://doi.org/10.1007/s10708-013-9516-8>
9. Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, 6, 239–242. <https://doi.org/10.1007/s12599-014-0334-4>
10. Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3, 18–23. <https://doi.org/10.1016/j.mfglet.2014.12.001>
11. McKee, D. W., Clement, S. J., Almutairi, J., & Xu, J. (2018). Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems. *CAAI Transactions on Intelligence Technology*, 3(2), 75–82. <https://doi.org/10.1049/trit.2018.0010>
12. Mohanan, M. G., & Salgoankar, A. (2018). A survey of robotic motion planning in dynamic environments. *Robotics and Autonomous Systems*, 100, 171–185. <https://doi.org/10.1016/j.robot.2017.10.011>
13. Monostori, L. (2014). Cyber-physical production systems: Roots, expectations and R&D challenges. *Procedia CIRP*, 17, 9–13. <https://doi.org/10.1016/j.procir.2014.03.115>
14. Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). Cyber-physical systems: The next computing revolution. In *Proceedings of the 47th Design Automation Conference* (pp. 731–736). ACM. <https://doi.org/10.1145/1837274.1837461>
15. Stone, P., & Veloso, M. (2000). Multiagent systems: A survey from a machine learning perspective. *Autonomous Robots*, 8, 345–383. <https://doi.org/10.1023/A:1008942012299>
16. Siciliano, B., & Khatib, O. (Eds.). (2016). *Springer handbook of robotics* (2nd ed.). Springer. <https://doi.org/10.1007/978-3-319-32552-1>
17. Siow, E., Tiropanis, T., & Hall, W. (2018). Analytics for the Internet of Things: A survey. *ACM Computing Surveys*, 51(4), Article 74, 1–36. <https://doi.org/10.1145/3204947>
18. Wang, L., Törngren, M., & Onori, M. (2015). Current status and advancement of cyber-physical systems in manufacturing. *Journal of Manufacturing Systems*, 37, 517–527. <https://doi.org/10.1016/j.jmsy.2015.04.008>
19. Xu, H., Yu, W., Griffith, D. W., & Golmie, N. T. (2018). A survey on industrial Internet of Things: A cyber-physical systems perspective. *IEEE Access*, 6, 78238–78259. <https://doi.org/10.1109/ACCESS.2018.2884906>
20. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. *IEEE Internet of Things Journal*, 1(1), 22–32. <https://doi.org/10.1109/IIOT.2014.2306328>