Evaluating the Impact of Agentic AI on Smart Technology in Autonomous Advanced Environment

Shital Pashankar[1]
Assistant Professor, School of Information Technology Indira University, Pune

Dr. Jyoti Jadhav[2]
Assistant Professor, School of Information Technology Indira University, Pune

Dr. Deven Mahajan[3]
Assistant Professor, School of Information Technology Indira University, Pune

DOI: 10.29322/IJSRP.16.02.2026.p17036
https://dx.doi.org/10.29322/IJSRP.16.02.2026.p17036

Paper Received Date: 9th January 2026
Paper Acceptance Date: 7th February 2026
Paper Publication Date: 12th February 2026

Abstract

Agentic AI is an artificial intelligence that can perform challenging tasks with little human help. Unlike older AI which has to face strict regulations and constant monitoring, agentic AI is capable of making its own advanced decisions, adapting to new situations, and acting freely in a dynamic environment. The key principles and methods of Agentic AI are discussed in detail in the current paper, as well as its unique ability to be self-sufficient and adjustable using LLM. We emphasize the applicability of the agentic systems in real-life situations with references to the thrilling prospects in the applications of these systems in such areas as software which must develop on its own, medicine, and finance. The questionnaire ends with the discussion of the serious ethical concerns that were brought forth by this technology, including the need to check whether the AI will be able to operate within the limits of the resources and whether its goals coincide with our own. To ensure that the transformative power of Agentic AI is used responsibly, it provides a framework of the safe implementation of the former in the society.

Index Terms - Agentic AI, LLM

INTRODUCTION

Agentic AI consists of limited and specialized tools to advanced AI agents who perceive, reason, and act under feedback of the surrounding environment. It has been stimulated by the development of Large Language Models (LLMs) which have caused individual agents to behave more complexly since they are now a strong foundation model, enhanced with modules that access memory, plan and use tools. Nevertheless, although single-agent architectures are approaching the point of failure in addressing the real-world demands, which demand an enormous diversity of skills, their concurrent execution, and coordinated effort, it is natural that more attention has turned to multi-agent systems. These consist of groups of expert agents, which work together, effectively handling issues which a single agent would not have been able to handle individually. The qualitative improvement of the older models of artificial intelligence is agentic AI; simply stated, it is an AI whose behavior involves creating and striving to achieve complex purposes in an uncontrollable, dynamic world, where it manages its own resources. As opposed to traditional AI models, which operate under the guidance of the human controller and execute only predetermined functions, Agentic AIs persist in supporting the goals and are constrained by the extent to which they are fed chaos as well as the necessity to alternate between the goals at the same time. This transition is informed by the dire need to come up with instruments that work effectively and efficiently in the real life that is often chaotic such as rescue operations in the wake of a natural disaster, medical delivery, and cyber security where autonomous and optimal decision making is necessary. The use of AI as assistant tools will finally be transformed into agentic AIs that can work together with the human equivalents to redistribute the workload and handle risky tasks to transform the work breakdown structure of the leading industry. Additionally agentic AI systems are being used more widely across different technologies and fields, including education, where they help support smarter decision-making and improve learning activities [7]. AI-powered learning tools improve both learning experience and efficiency in computer science students by offering quick and accurate assistance [6].

LITERATURE REVIEW

This literature review follows the development of AI as a strict, rule-driven system to Generative AI, and further into the framework of a free-will system, known as Agentic AI, which is characterized by the capacity to make its independent choices and move towards the accomplishment of certain objectives in dynamic environments. The review identifies key research gaps in scalability, real-time learning, and ethics and identifies the difference between Agentic AI and its predecessors by analyzing such architectures as multi-agent systems, hierarchical reinforcement learning, etc. It emphasizes the necessity of including safety governance and bias mitigation strategies to ensure that the same autonomous systems are launched into service in a responsible way [3]. The paper examines the use of AI in other fields of healthcare, robotics, and customer services and recommends that there is a clear distinction between basic and sophisticated systems. Whereas normal AI agents are optimally applied in simple, tool-based jobs such as catboats or schedule management, Agentic AI is aimed at far more autonomy and challenging jobs. This sophisticated version is capable of running its own objectives and integrating with other systems which is why it is suitable in high level applications such as medical decision making, science research or managing a set of robots who must coordinate without needing human intervention all the time [2]. In addition to improving cognitive skills, AI chatbots help increase learning efficiency by saving time and reducing effort.

The traditional AI solutions automate mundane tasks. The authors in this paper define the agentic system as one which can interact across service processes to a certain degree of self-direction, incorporating data inputs, decision making and producing operational outputs. The paper highlights the aspect of operational efficiency, personalization of guest services and strategic decision support played by agentic agents is also noted in this paper. It is found that AI-powered chatbots improve learning efficiency of students by providing personalized responses based on their needs [6]. In hospitality organizations as they introduce the opportunities of agentic AI. In the case of the hospitalization, the lid and the tourism industry, the author carefully discusses the issue of practical and ethical concerns with deployment. The paper also demonstrates that the successful adaptation will not only be based on Technological capability, but also on the organizational readiness, skills gaps and customer trust factors. The paper focuses on what are underdeveloped in the currently existing research. The paper comes up with research agenda that should be employed in a socio-technical framework in order to guide the future research. It should also be applied to governance, regulations and human-machine interaction in the hospitality environment [1]. In this paper, author examines the architectural evaluation of large language models (LLM) based multi agent systems (MAS) and their practical application across diverse application domains. It focuses on how multiple Alarm Power specialized agent can be organized into collaborative networks. These networks. Are capable of handling complex tasks through explicit orchestration and communication mechanisms. This paper. Focuses on. Case studies spanning. Telecommunications Security. Heritage Assess Management. And utilities customer service automation [2].

The research helps to comprehend the impact of generative models on and disciplinary knowledge production, research, design and pedagogical practices in education contexts. The author highlights. Religion regarding the authenticity, trustworthiness, and credibility of AI supported educational deliverables. In the educational sciences, it wrote a word of caution that unrestrained usage of the generative tools may lead to, or promote, biases, spread wrong information, or mislead to the point that it becomes hard to differentiate between original thought and automated suggestion. Such areas as healthcare, hospitality and smart system begin adapting to advanced paradigms of AI. Whereas. The educational research provides a balance between the innovation and academic rigour and trust in the institution [3]. The present paper will concentrate on the new paradigm of AI-driven in silico twins (ISTs) high fidelity computational patient models aimed at providing precision medicine. These IST integrate with physiological simulation which are data-driven and adaptive components. It comprises the valuation of the digital health technologies. Integrating the multimodal sources of data such as electronic health records, wearable sensors, imaging and omics profiles, therapy outcomes, etc. Technical taxonomy of ISTR architecture and its parts of operation was also discussed in the paper. It informs us of the way these elements are put together to facilitate adaptive simulation and patient care continuum decision support. The challenges and limitations are also less and they are; problem of model validation, cost of computation, privacy and incorporation of data within clinical workflow [4].The practical integration of interactive conversational agents within case-based research workflows is shown in this paper. This paper consists of how the generative models can be evaluated as interactive resource assistance which supports this case data. The author. Shows how researchers can use this as interface to reformulate research questions, find out anomalies in qualitative data, to find out insights without excessive manual retrieval. [5].

SIGNIFICANCE OF AGENTIC BASED ARTIFICIAL INTELLIGENCE TECHNIQUES

The agentic AI systems represent a viable extension of artificial intelligence whereby the agentic system is proven to be an independent decision-maker, a goal-oriented agent, and continues to learn in the dynamic environments. More to the point, Agentic AI is able to modify its functionality based on real-time information and shifting objectives, which is not typical of other types of AI, which tend to require some sort of human intervention or predefined and preprogrammed functions. The effectiveness and flexibility of such agents is yet again due to intelligence so that they employ most recent techniques, including machine learning, reinforcement learning, and the adoption of advanced multi-agent integration strategies. Using agentic AI in healthcare IoT systems creates serious security and privacy concerns, especially when handling sensitive patient data [9].

The Model Context Protocol (MCP) reference architecture is a very flexible and modular ecosystem, which is supposed to organize the various intelligent agents within various operating settings. In essence, a flexible deployment model is provided by the architecture to the organizations that choose it, allowing them to make trade-offs between latency, privacy and computational power; this would be realized via on-site and time-sensitive model deployments, cloud-based compute-intensive model deployments or the development of hybrid models that are able to adjust workloads on-the-fly to meet real-time needs. The framework expands the abilities of general-purpose Large Language Models (LLMs) with Specialized Function Agents. These dedicated units generate high-precision output by using specific algorithmic tools such as classical planning, mathematical optimization and computer vision. These specialized agents can easily be adapted to the larger ecosystem by customized adapters that encode internal logic into MCP-compliant interfaces. To sustain compatibility of this new structure with the existing structure, Legacy System Agents are sophisticated wrappers, protocols and state consistency translation are applied to overcome the existing APIs and the new agentic standard, and make certain high-stakes decisions are within the control of human beings. These various types of agents are combined in 4 important ways. patterns: hierarchical integration in order to structure command and control, peer-to-peer integration in order to work directly, service-oriented integration in order to discover in a modular way, and event-driven integration in order to react to stateful workflows. Together, these elements form an integrated, scalable architecture that enables architectural interoperability and enables the maximum specialization of each of the different components.

Pattern of Agent	Function	Advantages
Hierarchical	A complex task is decomposed in to Simpler e.g., a "Manager" agent delegating to "Coder" and "Tester" agents	Clear accountability, structured reasoning and predictable command flow.
Peer-to-peer	Rapid and direct collaboration between equal agents e.g., two specialized sensors swapping data	Low latency, highly flexible, decentralized with no single point of failure.
Service Oriented	Modular tools and reusable resources. e.g., a translation service used by variety of agents.	High reusability, standard interfaces, clear discovery through registries.
Event-driven	Real-time, reactive systems e.g., a "Security Agent" reacting instantly to a "Log Entry" event	Highly scalable and decoupled

MAJOR AGENTIC AI APPLICATIONS IN MULTIPLE DOMAINS

In the new healthcare reality, Agentic AI has not remained the very simplistic tool but has become a sophisticated clinical companion with data-intensive processes and hyper-personalized [4] data regarding patients. In contrast with old-fashioned software, these autonomous agents collaborate actively with clinicians by organizing the complex activities such as the high-speed and high-accurate division of medical imaging such as MRIs and CT scans and the real-time monitoring of physiological data to anticipate critical and time-sensitive phenomena such as seizures. In addition to the diagnostics, these systems are re-establishing the frontiers of personalized medicine, according to Lee. Through the state-of-the-art execution of genomic indicators, AI agents are in a position to anticipate susceptibility to ailments and store customized treatment protocols or timetables of disease flow according to an individual's distinctive genetic make-up and composition. This level of customization is further increased with the use of Multimodal multi-agent systems, whereby synthetic biometric feedback is used to create "digital twins". These virtual representations of the patient makes it possible to offer adaptive fitness and nutrition coaching that changes dynamically for how the user responds physiologically using realtime connected monitoring. 12 Agentic AI The delivery of Agentic AI is used in more specialized niches such in Neuromuscular Electrodiagnostic (EDX) testing using Retrieval-Augmented Generation (RAG) for the interpretation of complex test results. This is so that not only are each report standardized but they are highly based on the most current peer-reviewed medical literature to minimize human error and variability. Furthermore, the effects of these agents reach the basic levels of the application of medicine with the possibility of optimizing in drug discovery and surgical planning. In all these processes, integrated bioethical frameworks help to keep autonomous decision kept on track with strong medical ethics in between speed as a technical AND accountability as human.

In today's contest of high stakeholders in protracted warfare and digital defense, Agentic AI is enabling a way of thinking knowingly in mind-shifting paradigm in the need of our collective autonomy in which systems work in concerted "swarms" to neutralize threats that would overwhelm human mental capacity. These intelligent agents do not follow static and pre-programmed scripts rather they are decentralized units which can perform intricate offensive and defensive maneuvers. By processing huge

amounts of environmental information such swarms are able to take collective decisions in real time and can therefore dynamically change their tactics to the changing conditions of a physical battlefield or a digital network. This level of self-organization has given and will continue to provide mission objectives are achieved with a level of resilience and fleetness that is impossible under the command and control structures currently in place.

On the tactical front military agents are greeted with the capacity to optimally choose among the formations they will take and change their movements depending on a range of real-time performance indicators and threats to their situation. Whether on guard in a strategic location or conducting an orchestrated assault, these agents evaluate the most efficient journey moving forward, to assure continuity of operations even in the communications denied environment. This autonomy continues to spread into the field of Active Cyber Defense, especially in the cloud architecture, that is to say, in the area of cloud infrastructure. Whereas, to reduce the "attack surface" of a system, there is the potential of agents to rapidly change (in milliseconds) active services, reconfigure network topologies and change system parameters that could possibly be used to thwart sophisticated cyber-attacks. The integration of Automated Response protocols enables these agents to be used as the first line of defense against sophisticated cyber threats.

CHALLENGES IN DEPLOYING MULTI AGENT SYSTEM USING ARTIFICIAL INTELLIGENCE TECHNIQUES

While the vision of a self-optimizing "living grid" has an immensely much promise the move toward fully autonomous Multi-Agent Systems (MAS) is stifled by a number of formidable technical and systemic barriers. Primary amongst this are the Communication and Latency Overhead is a characteristic of the large-scale deployments. Upon increasing the density of agent network, the amount of inter agent data exchange which is exponential not linear Maintaining ultra-low in latency-- entry in to public grid systems qualified by authorities is ultimate non-negotiable prerequisite for safety consider essential tasks such as collision avoidance and signal synchronization. In the absence of ubiquitous and unfailing 5G coverage or 6G coverage: threat of "information lag" toward destabilizing the real time co-ordination broken in the water infrastructure management. In addition, the decentralized nature of these systems require complex Conflict Resolution and Arbitration protocols. In any complex urban environment, individual agents tend to have divergent or competing purposes; for instance, an emergency response agent would be required to put more emphasis on path clearing and velocity, whereas a public Every bus manager's first priority is energy saving and passenger stability, so there is an optimal question in the design of the transit agent. Without a robust, hierarchical arbitration logic to arbitrate between these conflicting goals, the network runs the risk of descending into a state of digital deadlock, where a competition of autonomous decision, leading to systemic paralysis; This is augmented by the phenomenon of Emergent Behaviors where the interaction of hundreds of independent agents create unexpected patterns implicitly left out of the code by developers. While some emergent traits may be more efficient, others can take the form of unpredictable system failures which will require rigorous simulation-native testing to ensure the grid will remain predictable under stress.

Finally, Integration Agentic AI carries very big Cyber-Physical Security risks with it. Because these agents are so subsumed in their physical infrastructure, a single compromised node can be a catastrophic point of attack by malicious actors, allowing for the unauthorized manipulation of traffic signals, power grids or logistics hubs. To counter this developer must go beyond normative firewalls towards a decentralized trust frames and automated circuit breakers. These security measures are designed to identify anomalous activity by agents instantaneously. Also immediately quarantine infected units in order to ensure that a localized breach does not have a chance to spread. According to [8] the adoption of agentic AI differs across fields because some areas are more prepared, while others are hesitant due to security concerns.

CONCLUSION

Finally, Integration Agentic AI carries very big Cyber-Physical Security risks with it. Because these agents are so subsumed in their physical infrastructure, a single compromised node can be a catastrophic point of attack by malicious actors, allowing for the unauthorized manipulation of traffic signals, power grids or logistics hubs. To counter this, developer must go beyond normative firewalls towards a decentralized trust frames and automated circuit breakers. These security measures are designed to identify anomalous activity by agents instantaneously and immediately quarantine infected units, in order to ensure that a localized breach does not have a chance to spread.

REFERENCES

1. Dwivedi, Y. K., Helal, M. Y. I., Elgendy, I. A., Albashrawi, M. A., Hughes, L., Shawosh, M., ... & Jeon, I. (2026). Artificial intelligence agents and agentic systems in hospitality and tourism: challenges, opportunities and research agenda. International Journal of Contemporary Hospitality Management, 38(1), 27-52.
2. Banerjee, S. (2026, December). Historical Genealogies of Data Colonialism: From Colonial Censuses to Digital AI Systems. In International Conference on Smart Systems and Social Management (ICSSSM-2 2025) (pp. 991-1004). Atlantis Press.
3. Brezovec, E., Zelić, M., & Zagode, A. M. (2026). Stabilizing truth in educational sciences: a systematic review of generative AI in education. Kybernetes, 55(13), 1-17.
4. Alharthi, S. (2026). AI-powered in silico twins: redefining precision medicine through simulation, personalization, and predictive healthcare. Saudi Pharmaceutical Journal, 34(1),
5. Heinbach, C. (2026). Chat with my case study. Informatik Spektrum, 1-13.
6. Shankar, P., Murali, J., Das, S., Shinde, A., & Tekriwal, M. (2024, December). AI-Powered Learning: Exploring the Dual Impact of Generative AI Chatbots on Enhancing Cognitive Skills and Efficiency Amongst Computer Science Learners. In International Conference on Technology 4 Education (pp. 166-176). Singapore: Springer Nature Singapore.
7. Tran, G. T., Le Dinh, T., & Le, T. D. (2026). Agentic AI Across Technologies, Applications, and Development Domains: A Systematic Literature Review. In International Conference on Data Analytics & Management (pp. 587-601). Springer, Cham.
8. Waizel, G. (2026). The Agentic AI Security Adoption Matrix: Understanding Readiness and Resistance Across Domains.
9. Adil, M., Ali, A., Hakim, S. B., Farouk, A., Abulkasim, H., Khan, M. K., & Song, H. (2026). Security and Privacy Challenges in Healthcare Internet of Things Applications in the Era of Agentic AI. Authorea Preprints.