International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJARCST.2025.0805036

Transforming Cloud Native Enterprise Systems with Agentic Artificial Intelligence and Intelligent Automation Frameworks

Geetha Varsha Chandrasekar

Senior Software Developer, Nasdaq, Canada

ABSTRACT: Cloud-native enterprise systems have rapidly evolved from monolithic architectures to distributed, containerized, and microservices-driven ecosystems deployed across hybrid and multi-cloud environments. Despite these advancements, enterprises continue to face challenges such as operational complexity, dynamic scaling inefficiencies, observability gaps, and increasing security risks. This paper explores the transformation of cloud-native enterprise systems through the integration of agentic artificial intelligence and intelligent automation frameworks. Agentic AI introduces autonomous, goal-driven software agents capable of perceiving system states, reasoning over contextual data, and executing adaptive actions without continuous human intervention. When combined with intelligent automation frameworks, these agents enable self-healing infrastructures, predictive scaling, autonomous incident response, and continuous optimization of workloads. The study examines how these technologies collectively shift enterprise cloud operations from reactive and rule-based models to proactive, adaptive, and self-governing systems. It further analyzes architectural patterns that support agent orchestration, reinforcement learning-driven optimization loops, and event-driven automation pipelines. By synthesizing current research and emerging industrial practices, this paper highlights the potential of agentic AI to redefine DevOps, SRE (Site Reliability Engineering), and cloud governance paradigms. The findings suggest that enterprises adopting these frameworks can achieve higher system resilience, reduced operational overhead, improved cost efficiency, and accelerated innovation cycles, while also introducing new challenges in trust, explainability, and control mechanisms.

KEYWORDS: Agentic AI, Cloud-Native Systems, Intelligent Automation, Microservices, DevOps, Self-Healing Systems, Multi-Cloud, Kubernetes, Autonomous Agents, AIOps

I. INTRODUCTION

The evolution of enterprise computing has undergone several paradigm shifts, moving from centralized mainframe systems to distributed client-server architectures and eventually to cloud computing models. In recent years, cloud-native systems have emerged as the dominant architecture for building scalable, resilient, and flexible enterprise applications. These systems leverage microservices, containerization, and orchestration platforms such as Kubernetes to enable rapid deployment and dynamic scaling across heterogeneous environments. However, as enterprise systems grow in scale and complexity, traditional automation and monitoring approaches have proven insufficient to manage the increasing operational burden.

Cloud-native ecosystems are inherently dynamic, characterized by ephemeral workloads, continuous deployment pipelines, and distributed service interactions. This complexity introduces challenges in observability, fault tolerance, resource optimization, and security management. Human-driven operations and static rule-based automation systems often struggle to keep pace with real-time system changes. As a result, organizations are increasingly exploring artificial intelligence-driven solutions to enhance operational intelligence and reduce manual intervention.
Agentic artificial intelligence represents a significant advancement beyond conventional machine learning and automation techniques. Unlike traditional AI systems that passively respond to inputs, agentic AI systems are designed to act autonomously, pursue objectives, and adapt their behavior based on environmental feedback. These agents can interact with cloud infrastructure, analyze telemetry data, detect anomalies, and execute corrective actions in real time. When integrated into cloud-native environments, they enable a shift from human-in-the-loop operations to AI-augmented or even AI-autonomous systems.

Intelligent automation frameworks complement agentic AI by providing structured orchestration layers, workflow automation pipelines, and decision execution mechanisms. Together, these technologies facilitate the emergence of

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJARCST.2025.0805036

self-managing enterprise systems capable of self-healing, self-optimizing, and self-configuring behaviors. This transformation aligns with the broader vision of autonomous computing, where systems continuously adapt to changing workloads and business requirements without explicit human intervention.

This paper explores the intersection of cloud-native enterprise systems, agentic AI, and intelligent automation frameworks. It investigates how these technologies collectively reshape system architecture, operational models, and governance strategies. It also examines the implications of adopting such systems, including challenges related to transparency, reliability, ethical decision-making, and system accountability.

II. LITERATURE REVIEW

Recent advancements in cloud computing have emphasized the transition toward cloud-native architectures, which prioritize scalability, resilience, and modularity. Research in this domain highlights the role of microservices in decomposing monolithic applications into independently deployable components, enabling faster development cycles and improved fault isolation. Container orchestration platforms such as Kubernetes have become foundational in managing these distributed workloads, providing automated scheduling, scaling, and recovery mechanisms.

Parallel to these developments, the field of Artificial Intelligence for IT Operations (AIOps) has emerged as a key area of research. AIOps focuses on applying machine learning techniques to IT operations data in order to detect anomalies, correlate events, and automate incident response. Early AIOps systems relied heavily on supervised learning models trained on historical logs and metrics. However, these systems often lacked adaptability in highly dynamic environments, limiting their effectiveness in real-time decision-making scenarios.

The concept of autonomous systems in computing has been explored through the lens of autonomic computing, which defines self-managing systems capable of self-configuration, self-healing, self-optimization, and self-protection. While autonomic computing laid the theoretical foundation for self-managing systems, its practical implementation was constrained by limited AI capabilities at the time.

More recent research has introduced the concept of agent-based systems, where software agents operate with a degree of autonomy, interacting with their environment and other agents to achieve defined objectives. These agents have been applied in distributed computing, network management, and cloud resource optimization. However, most existing implementations remain rule-based or narrowly scoped, lacking the full cognitive capabilities associated with modern large language model-driven agents.

The emergence of large language models and reinforcement learning-based systems has enabled the development of more sophisticated agentic AI frameworks. These agents can interpret unstructured data, reason across multi-step problems, and execute complex workflows by interacting with external tools and APIs. Studies have shown that such systems can significantly improve decision-making speed and accuracy in operational environments.

Intelligent automation frameworks have also evolved significantly, integrating robotic process automation with AI-driven decision engines. These frameworks enable end-to-end workflow automation across enterprise systems, reducing manual intervention and improving operational efficiency. However, integration with cloud-native systems remains a challenge due to the distributed and highly dynamic nature of modern infrastructures.

The convergence of these fields suggests a new paradigm in enterprise computing, where cloud-native systems are no longer merely automated but are increasingly autonomous. Research indicates that integrating agentic AI with intelligent automation can lead to improved system resilience, reduced downtime, and optimized resource utilization. Nevertheless, concerns remain regarding system transparency, control, security vulnerabilities, and the ethical implications of autonomous decision-making.

III. RESEARCH METHODOLOGY

The research methodology adopted in this study is designed to analyze the transformation of cloud-native enterprise systems through the integration of agentic artificial intelligence and intelligent automation frameworks. The approach is primarily qualitative, supported by conceptual architectural analysis and secondary data synthesis from existing literature, industry reports, and documented case studies in cloud computing and AI-driven operations. The

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJARCST.2025.0805036

methodology is structured to provide a comprehensive understanding of system behavior, architectural evolution, and operational implications.

The first phase of the methodology involves a systematic conceptual analysis of cloud-native architectures. This includes examining microservices-based design patterns, container orchestration mechanisms, service mesh architectures, and event-driven communication models. The objective is to identify key operational challenges such as service latency, inter-service dependency complexity, fault propagation, and scaling inefficiencies. This phase establishes the baseline understanding of traditional cloud-native systems without AI augmentation. The second phase focuses on the analysis of agentic AI systems. This involves studying the characteristics of autonomous agents, including perception, reasoning, planning, and action execution. Particular emphasis is placed on how these agents utilize reinforcement learning, large language models, and tool-augmented reasoning to interact with external systems. The analysis also considers multi-agent coordination strategies, where multiple autonomous agents collaborate to achieve system-wide objectives such as load balancing, anomaly resolution, or cost optimization.

The third phase examines intelligent automation frameworks and their role in enterprise environments. This includes workflow orchestration engines, robotic process automation systems, event-driven automation pipelines, and policy-based decision systems. The study analyzes how these frameworks integrate with existing IT operations to automate repetitive tasks, enforce compliance policies, and streamline incident management processes. The interoperability between automation frameworks and cloud-native infrastructure components is a key focus area. The fourth phase involves the synthesis of integration architectures that combine cloud-native systems, agentic AI, and intelligent automation. Several architectural models are evaluated conceptually, including centralized agent control models, decentralized multi-agent ecosystems, and hybrid human-AI collaborative frameworks. These models are analyzed based on scalability, resilience, latency, fault tolerance, and governance complexity. The goal is to identify optimal integration patterns that maximize operational efficiency while minimizing systemic risks.

The fifth phase explores data flow and feedback loop mechanisms within agentic cloud-native environments. In these systems, telemetry data such as logs, metrics, traces, and events are continuously collected and fed into AI agents. These agents analyze system state, detect anomalies, and initiate corrective actions through automation frameworks. The feedback loop is iterative, enabling continuous learning and adaptation. The methodology examines how closed-loop control systems enhance system stability and performance optimization over time. The sixth phase focuses on simulation-based reasoning. Hypothetical enterprise scenarios are constructed to evaluate how agentic AI systems respond to real-world operational challenges such as traffic spikes, service outages, security breaches, and resource contention. These scenarios are used to assess decision-making efficiency, recovery time, and system resilience. Although not experimentally implemented, these simulations are grounded in documented industry behaviors and theoretical models. The seventh phase addresses governance, security, and ethical considerations. The methodology evaluates how autonomous decision-making systems can be monitored, controlled, and audited. It examines the role of explainability frameworks, policy enforcement engines, and human-in-the-loop oversight mechanisms. Particular attention is given to risks such as unintended system behavior, cascading failures, and adversarial manipulation of AI agents.

The final phase synthesizes findings into a unified conceptual framework that describes the transformation of cloud-native enterprise systems into agentic, self-managing ecosystems. This framework highlights the transition from reactive monitoring to proactive autonomy, emphasizing the role of continuous intelligence in system operations. It also identifies gaps in current research, particularly in the areas of trust calibration, multi-agent coordination at scale, and real-time governance enforcement. Overall, the methodology combines theoretical analysis, system modeling, and conceptual synthesis to provide a comprehensive understanding of how agentic AI and intelligent automation are reshaping cloud-native enterprise systems. It establishes a foundation for future empirical research and practical implementation strategies aimed at achieving fully autonomous cloud operations.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJARCST.2025.0805036

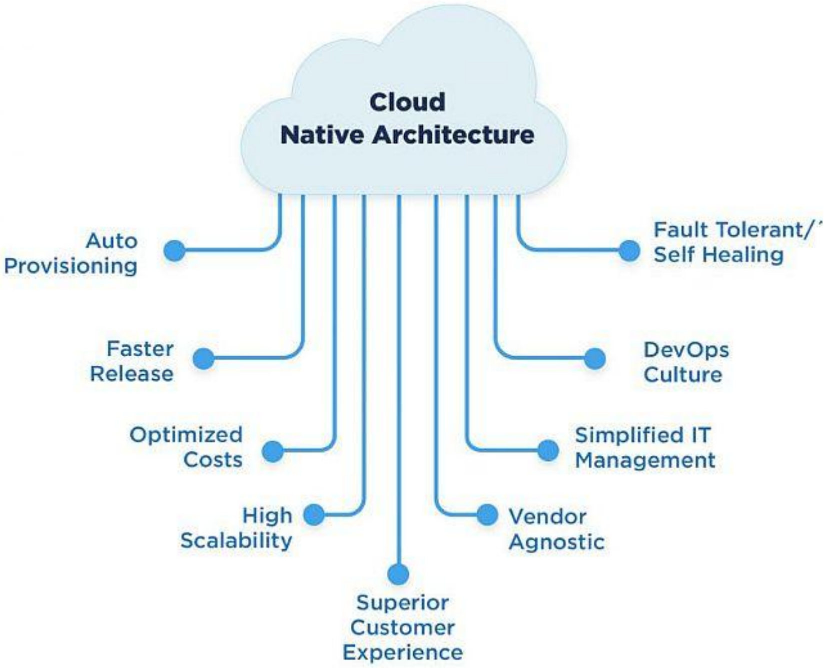

Fig.1.How Cloud Native is Transforming Enterprise IT

REFERENCES

1. Mohammed, S., & Polamarasetty, V. K. (2023). Azure cloud landing zone architecture for enterprise-scale cloud adoption. International Journal of Information Technology and Management Information Systems, 14(1), 117–147. https://doi.org/10.34218/IJITMIS_14_01_012
2. Meesala, L. K. (2023). A layered security framework for enterprise operations in the Generative AI and Agentic AI era in regulated cloud environments. International Journal of Future Innovative Science and Technology (IJFIST), 6(6), 11752–11760.
3. Sudakara, B. B. (2023). Integrating Cloud-Native Testing Frameworks with DevOps Pipelines for Healthcare Applications. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(5), 9309-9316.
4. Gurram, S. K. (2024). Federated learning for anomaly detection in distributed systems. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 14031–14040.
5. Chettiyar, S. S. S. (2024). Agentic AI orchestrated conversational payment pipelines with drift-aware transaction. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(3), 8166–8174. https://doi.org/10.15662/IJEETR.2024.0603008
6. Devineni, A. (2023). Automated Compliance-Driven Patch Management and Security Hardening in Multi-Cloud Banking Infrastructure Using IaC and Python Orchestration. The American Journal of ET, 5(12), 68-80.
7. Govindan, V. (2024). Automating vulnerability remediation: A continuous SAST and FOSS integration framework for production support pipelines. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7899–7916. https://doi.org/10.15662/IJEETR.2024.0602014
8. Kanchumarthi, S. N. V. P. (2024, April). Hybrid network security architecture: F5–AWS integration, zero-trust enforcement, and SD-WAN for PCI DSS-compliant hybrid environments. World Journal of Advanced Research and Reviews, 22(1), 2111–2117. https://doi.org/10.30574/wjarr.2024.22.1.1162
9. Sarngadharan, S. (2024). A secure, zero-trust mobile expert locator for global professional services firms. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(3), 8157–8165. https://doi.org/10.15662/IJEETR.2024.0603007
10. Mannem, S. (2024). From requirements to production: Managing cross-regional API deployments at Capital One. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7892–7898. https://doi.org/10.15662/IJEETR.2024.0602013

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJARCST.2025.0805036

11. Gandikota, S. P. (2024). Scaling national wireless services: A technical case study of T-Mobile's middleware evolution on AWS cloud. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7869–7877. https://doi.org/10.15662/IJEETR.2024.0602011
12. Syed, S. (2024). A zero-defect high sea sale automation framework for real-time ownership transfer and compliance in maritime trade systems. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7878–7891. https://doi.org/10.15662/IJEETR.2024.0602012
13. Chenna, S. (2024). Reinforcement learning-based dynamic load assignment for automated 3PL tendering systems. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7917–7932. https://doi.org/10.15662/IJEETR.2024.0602015
14. Polamreddy, V. R. (2024). Hybrid On-Premise to Cloud Data Migration: Architectural Patterns for Controlled One-Way Synchronization. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(3), 8143-8156.
15. Kotla, M. R. T. (2024). Optimizing enterprise integration pipelines using cloud-native data engineering and middleware solutions. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(5), 11311-11314.
16. Manda, P. (2024). The role of machine learning in automating complex database migration workflows. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(3), 10451–10459.
17. Makkena, B. (2023). PromptOps: Building prompt-driven DevOps workflows for infrastructure-as-code automation. International Journal of Communication Networks and Information Security, 15(10), 12–30.
18. Adari, V. K. (2024). Interoperability and Data Modernization: Building a Connected Banking Ecosystem. International Journal of Computer Engineering and Technology (IJCET), 15(6), 653-662.
19. Dama, H. B. (2024). Cross-Cloud Data Consistency Models for Always-On Banking Platforms. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8468-8476.
20. Anumula, S. K. (2025). Next-gen supply chains: A product lifecycle management–based approach to resilient and sustainable operations. International Journal of Managing Value and Supply Chains (IJMVSC), 16.
21. Juvvadi, R. R. (2019). Smart contracts in supply chain finance: Automating accounts payable and the three-way match. Journal of Information Systems Engineering and Management, 4(1), 1–12.
22. Sharma, Ankit and Mulgund, Pavankumar and Srivastava, Adarsh and Agrawal, Lavlin, Beyond Cryptocurrency: There’s More to Blockchain (January 07, 2020). Beyond Cryptocurrency: There's More to Blockchain," Amplify, Cutter Consortium, January 7, 2020., Available at SSRN: https://ssrn.com/abstract=6098906 or http://dx.doi.org/10.2139/ssrn.6098906
23. Mathew, A., & Mai, C. (2018, May). Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 2021-2024). IEEE.
24. Sunnam, S. V. B. R. (2021). Big Data Analytics Using Hadoop and Spark: Applications, Challenges, and Future Direction. Journal of Computer Science and Technology Studies, 3(1), 50-62.
25. Soundappan, S. J. (2021). DataOps: Orchestrating Reliable ML Data Pipelines. International Journal of Research and Applied Innovations, 4(4), 5533-5537.
26. Devineni, A. (2022). Proactive incident detection in multi-tenant financial cloud platforms. International Journal of Science, Research and Technology, 5(4), 8136-8139.
27. Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.
28. Raj, A. A., & Sugumar, R. (2022, December). Monitoring of the Social Distance between Passengers in Real-time through Video Analytics and Deep Learning in Railway Stations for Developing the Highest Efficiency. In 2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (Vol. 1, pp. 1-7). IEEE.
29. Raja, G. V. (2020). Metadata gets a makeover: The machine learning approach. International Journal of Computer Technology and Electronics Communication, 3(6), 2900-2903.
30. Parasa, M. (2023). A structured recruitment analytics framework for candidate screening and talent pool utilization in SAP SuccessFactors Recruiting. Global Journal of Engineering and Technology, 2(11), 29–39. https://gsarpublishers.com/gjet-vol-2-issue-11-november-2023/
31. Navandar, P. (2024). Governance, risk, and compliance (GRC) in the age of identity and access governance (IAG): A framework for integrated enterprise security and compliance. International Journal of Research and Applied Innovations (IJRAI), 7(2), 10483–10493. https://doi.org/10.15662/IJRAI.2024.0702011

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJARCST.2025.0805036

32. Meesala, A. (2022). Adaptive Spread Anomaly Intelligence Framework (ASAIF): A cloud-native AI framework for real-time bid-ask spread anomaly detection and cross-venue liquidity risk intelligence. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9597–9604.
33. Gupta, S., Barigidad, S., Hussain, S., Dubey, S., & Kanaujia, S. (2025, February). Hybrid Machine Learning for Feature-Based Spam Detection. In 2025 2nd International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 801-806). IEEE.
34. Gopisetty, S. (2024). Why was my transaction flagged? Building counterfactual stories for AI threat detection in real-time ERP systems. QIT Press - International Journal of Artificial Intelligence Research and Development (QITP-IJAIRD), 5(1), 20–56.
35. Prasad, P. K. (2024). Establishing AI governance frameworks within CloudOps to accelerate safe, compliant AI adoption at scale. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 14030.