International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 1, January-February 2026 |

DOI:10.15662/IJEETR.2026.0801023

Agentic AI Driven Enterprise Architecture for Secure Autonomous Decision Making and Continuous Compliance

Leslie Teo

AI Product Architect, AI Singapore, Singapore

ABSTRACT: The rapid advancement of artificial intelligence has transformed enterprise operations by enabling autonomous systems capable of making intelligent decisions with minimal human intervention. Agentic Artificial Intelligence (Agentic AI) represents a significant evolution beyond traditional AI by integrating autonomous reasoning, adaptive learning, goal-oriented planning, and continuous execution within enterprise environments. As organizations increasingly adopt digital transformation strategies, the integration of Agentic AI into Enterprise Architecture (EA) has emerged as a critical approach for improving operational efficiency, strengthening cybersecurity, enhancing governance, and ensuring continuous regulatory compliance. However, autonomous decision-making introduces challenges related to transparency, accountability, trust, data privacy, and regulatory adherence. This study explores the role of Agentic AI-driven Enterprise Architecture in facilitating secure autonomous decision-making while maintaining continuous compliance across complex organizational ecosystems. The research examines architectural frameworks, governance mechanisms, cybersecurity principles, compliance automation, and AI-driven risk management strategies that support resilient enterprise operations. A qualitative research methodology based on extensive literature analysis, industry frameworks, and comparative evaluation is employed to identify best practices and implementation challenges. The findings indicate that integrating intelligent autonomous agents with zero-trust security, explainable AI, continuous monitoring, policy automation, and governance frameworks significantly enhances enterprise resilience, operational agility, and regulatory compliance. The study concludes that Agentic AI-driven Enterprise Architecture provides a sustainable foundation for future intelligent enterprises operating in highly dynamic and regulated digital environments.

KEYWORDS: Agentic AI, Enterprise Architecture, Autonomous Decision Making, Continuous Compliance, Artificial Intelligence, Cybersecurity, Governance, Zero Trust Security, Explainable AI, Digital Transformation, Intelligent Agents, Risk Management, Regulatory Compliance, Enterprise Governance, Secure AI Systems

I. INTRODUCTION

Digital transformation has fundamentally reshaped modern organizations by introducing intelligent technologies capable of automating business operations, improving decision-making, and enhancing customer experiences. Artificial Intelligence (AI) has become one of the most influential technologies driving this transformation, enabling organizations to process large volumes of data, recognize complex patterns, and support strategic business decisions. Traditional AI systems primarily function as predictive or analytical tools that assist human decision-makers. However, the emergence of Agentic Artificial Intelligence represents a paradigm shift toward autonomous systems capable of independently planning, reasoning, adapting, and executing complex tasks with minimal human supervision. Unlike conventional AI models that operate within predefined boundaries, Agentic AI demonstrates goal-oriented behavior, contextual reasoning, memory, learning capabilities, and dynamic decision-making across interconnected enterprise environments.

The growing adoption of Agentic AI has significant implications for Enterprise Architecture (EA), which serves as the strategic blueprint aligning organizational objectives, business processes, information systems, technology infrastructure, and governance mechanisms. Enterprise Architecture enables organizations to maintain operational consistency while adapting to technological innovations and evolving business requirements. Integrating Agentic AI into Enterprise Architecture extends traditional architectural principles by embedding intelligent autonomous agents into business workflows, cybersecurity systems, governance structures, compliance monitoring, and decision-support processes. Such integration enables enterprises to achieve higher levels of automation, operational agility, and organizational resilience while maintaining alignment with strategic objectives.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 1, January-February 2026 |

DOI:10.15662/IJEETR.2026.0801023

Despite these advantages, the deployment of autonomous AI systems introduces several challenges that require careful architectural planning and governance. Autonomous decision-making may create risks associated with cybersecurity vulnerabilities, biased decision outcomes, privacy violations, regulatory non-compliance, explainability limitations, and ethical concerns. Organizations operating within highly regulated industries such as finance, healthcare, government, and critical infrastructure must ensure that autonomous AI systems comply with legal requirements, industry standards, and organizational policies throughout their operational lifecycle. Consequently, continuous compliance has emerged as a fundamental requirement for AI-enabled enterprises, requiring automated monitoring, real-time auditing, policy enforcement, and adaptive governance mechanisms.

Agentic AI-driven Enterprise Architecture addresses these challenges by integrating intelligent governance frameworks with secure architectural principles such as Zero Trust Security, Explainable AI, continuous risk assessment, policy automation, and AI lifecycle management. These architectural capabilities enable enterprises to monitor autonomous decision-making processes continuously while maintaining transparency, accountability, and regulatory compliance. Additionally, intelligent agents can proactively identify operational risks, detect security threats, recommend corrective actions, and automate compliance reporting across distributed enterprise systems.

The increasing complexity of enterprise ecosystems, characterized by cloud computing, Internet of Things devices, edge computing, multi-cloud environments, and distributed digital platforms, further emphasizes the need for adaptive architectural models capable of supporting secure autonomous operations. Agentic AI offers the capability to coordinate multiple intelligent agents across interconnected systems, enabling collaborative decision-making, dynamic resource allocation, predictive risk management, and continuous operational optimization.

This study investigates how Agentic AI-driven Enterprise Architecture enables secure autonomous decision-making while supporting continuous compliance within modern organizations. The research explores existing architectural frameworks, governance models, cybersecurity strategies, compliance automation techniques, and intelligent decision-support mechanisms. It further evaluates implementation challenges, organizational readiness factors, and future research opportunities, contributing to the development of trustworthy, resilient, and intelligent enterprise ecosystems capable of operating effectively within rapidly evolving digital environments.

II. LITERATURE REVIEW

The evolution of Enterprise Architecture has traditionally focused on aligning business strategy, information systems, technology infrastructure, and organizational governance to achieve operational efficiency and strategic agility. Established Enterprise Architecture frameworks have emphasized structured governance, standardized processes, interoperability, and business-technology alignment. However, the emergence of artificial intelligence has transformed Enterprise Architecture from a static planning discipline into an adaptive, intelligent, and continuously evolving ecosystem capable of autonomous optimization.

Recent literature identifies Agentic AI as the next generation of artificial intelligence characterized by autonomous reasoning, planning, memory, environmental awareness, and goal-directed behavior. Unlike conventional machine learning systems that primarily perform classification or prediction tasks, Agentic AI systems actively interact with their environments, formulate strategies, coordinate multiple agents, and continuously adapt to changing organizational conditions. Researchers argue that these capabilities make Agentic AI particularly suitable for enterprise-scale automation involving complex decision-making across interconnected business processes.

Several studies emphasize that secure autonomous decision-making requires integrating AI governance with cybersecurity principles throughout Enterprise Architecture. Zero Trust Security has gained considerable attention as an architectural approach that assumes no implicit trust within enterprise networks. Continuous authentication, least-privilege access control, identity verification, and micro-segmentation reduce security risks associated with autonomous AI agents operating across distributed enterprise environments.

The concept of continuous compliance has also received increasing scholarly attention due to evolving regulatory requirements and dynamic cybersecurity threats. Traditional compliance management often relies on periodic manual audits, resulting in delayed detection of policy violations and increased operational risks. Recent research advocates automated compliance monitoring using AI-enabled governance platforms capable of continuously assessing regulatory adherence, identifying compliance gaps, and generating real-time audit evidence. Agentic AI extends these capabilities

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 1, January-February 2026 |

DOI:10.15662/IJEETR.2026.0801023

by autonomously interpreting regulatory changes, updating organizational policies, monitoring system behavior, and recommending corrective actions without extensive human intervention.

Explainable Artificial Intelligence has emerged as another critical research area supporting trustworthy autonomous decision-making. Regulatory frameworks increasingly require organizations to justify AI-generated decisions affecting customers, employees, and stakeholders. Explainable AI techniques improve transparency by providing interpretable reasoning behind autonomous decisions, thereby enhancing accountability, stakeholder trust, and regulatory acceptance.

Researchers have also examined the integration of digital twins, knowledge graphs, multi-agent systems, and reinforcement learning into Enterprise Architecture. These technologies enable intelligent agents to model enterprise environments, simulate decision outcomes, optimize resource allocation, and coordinate complex organizational processes while minimizing operational risks. Multi-agent architectures further enhance scalability by distributing decision-making responsibilities among specialized autonomous agents operating collaboratively under centralized governance policies.
Despite substantial technological advancements, the literature consistently identifies several implementation challenges, including organizational resistance, data quality limitations, cybersecurity vulnerabilities, ethical concerns, governance complexity, interoperability issues, and workforce readiness. Existing studies recommend adopting hybrid governance models combining human oversight with autonomous AI decision-making to ensure responsible deployment. Furthermore, standardized AI governance frameworks, continuous monitoring mechanisms, lifecycle risk management, and adaptive security architectures are considered essential for sustainable implementation.

Overall, contemporary literature demonstrates growing consensus that Agentic AI-driven Enterprise Architecture has significant potential to transform enterprise operations by enabling intelligent automation, resilient cybersecurity, continuous compliance, and adaptive organizational governance. However, successful implementation depends on balancing autonomous capabilities with robust governance, transparency, ethical responsibility, and continuous human supervision to ensure secure and trustworthy enterprise ecosystems.

III. RESEARCH METHODOLOGY

This study adopts a qualitative research methodology to investigate the role of Agentic Artificial Intelligence-driven Enterprise Architecture in enabling secure autonomous decision-making and continuous compliance within modern organizations. A qualitative research approach is appropriate because the study focuses on understanding emerging technological concepts, architectural principles, governance mechanisms, organizational strategies, and implementation practices rather than measuring numerical relationships between predefined variables. Since Agentic AI is an evolving research domain with limited standardized implementation models, qualitative inquiry provides flexibility to explore conceptual frameworks, identify recurring patterns, synthesize interdisciplinary knowledge, and develop comprehensive insights from multiple scholarly perspectives.

The research follows an interpretivist philosophical paradigm, recognizing that enterprise architecture, artificial intelligence governance, cybersecurity, and compliance management are influenced by organizational contexts, stakeholder perspectives, technological maturity, and regulatory environments. The interpretivist approach enables a deeper understanding of how organizations design, implement, govern, and evaluate Agentic AI within enterprise ecosystems. Rather than seeking universal laws, the research aims to explain relationships among technological capabilities, governance structures, security controls, and compliance practices.

A descriptive research design is employed to examine the existing body of knowledge surrounding Agentic AI, Enterprise Architecture, cybersecurity, governance, and continuous compliance. The descriptive design allows systematic documentation of current architectural practices, emerging implementation strategies, security mechanisms, regulatory requirements, and organizational experiences. It further supports comparative analysis of different frameworks and identifies common architectural characteristics associated with successful AI adoption.

The study relies exclusively on secondary data collected from peer-reviewed journal articles, conference proceedings, books, industry reports, international standards, white papers, government publications, and recognized enterprise architecture frameworks. Sources are selected based on relevance, credibility, publication quality, and contribution to the research objectives. Particular emphasis is placed on publications discussing AI governance, enterprise architecture, autonomous systems, explainable AI, Zero Trust Architecture, cybersecurity, and regulatory compliance.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 1, January-February 2026 |

DOI:10.15662/IJEETR.2026.0801023

A systematic literature review process is adopted to ensure transparency, reproducibility, and comprehensive coverage of existing knowledge. Relevant databases such as IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Scopus, Web of Science, Google Scholar, and leading professional organizations are searched using combinations of keywords including "Agentic AI," "Enterprise Architecture," "Autonomous Decision Making," "Continuous Compliance," "AI Governance," "Zero Trust Security," "Explainable AI," "Cybersecurity Architecture," "Multi-Agent Systems," and "Digital Transformation." Inclusion criteria prioritize recent publications, foundational theoretical works, and highly cited research. Duplicate, non-peer-reviewed, and irrelevant publications are excluded after screening.

The collected literature undergoes thematic analysis to identify recurring concepts, implementation strategies, governance principles, security mechanisms, compliance models, organizational benefits, and research gaps. Coding procedures categorize information into themes such as autonomous decision-making, enterprise governance, AI lifecycle management, policy automation, risk management, security architecture, regulatory compliance, explainability, human oversight, and organizational transformation. These themes are compared across multiple studies to identify similarities, differences, emerging trends, and unresolved challenges.

To strengthen analytical rigor, triangulation is achieved through the integration of academic literature, industry best practices, international standards, and enterprise architecture frameworks. Cross-validation of evidence from multiple independent sources improves the credibility and reliability of research findings while minimizing individual source bias. The methodological process also incorporates critical evaluation of contrasting viewpoints regarding autonomous AI governance, ethical considerations, security risks, and organizational readiness.
The methodology further includes comparative framework analysis, examining prominent enterprise architecture models and AI governance approaches to assess their suitability for supporting Agentic AI. Architectural principles related to modularity, interoperability, scalability, resilience, policy enforcement, monitoring, auditing, and security are evaluated in relation to autonomous decision-making capabilities. Compliance frameworks and regulatory guidelines are analyzed to determine how automated governance mechanisms can support continuous monitoring and adaptive policy enforcement.

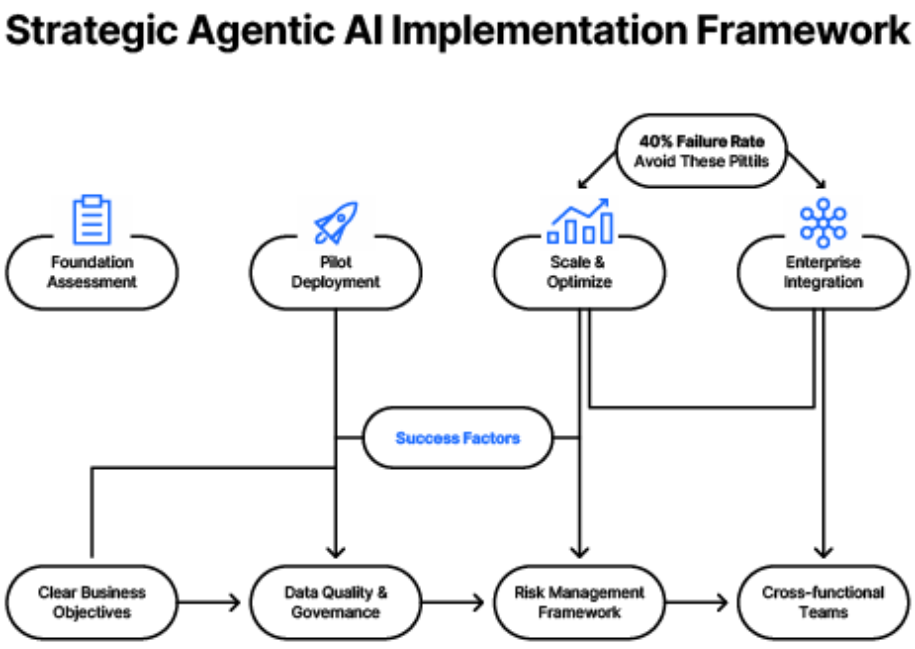

Fig.1. Strategic Agentic AI

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 1, January-February 2026 |

DOI:10.15662/IJEETR.2026.0801023

Ethical considerations are addressed by ensuring accurate representation of published findings, proper acknowledgment of original authors, avoidance of plagiarism, and objective interpretation of evidence. Since the study uses publicly available secondary sources and does not involve human participants or personal data, ethical risks are minimal.

The research acknowledges several limitations. The rapidly evolving nature of Agentic AI means that new technologies, standards, and regulations may emerge after the completion of the study. Additionally, because the research is based on secondary data, it cannot directly evaluate organizational implementation outcomes through empirical observation. Nevertheless, the synthesis of multidisciplinary evidence provides a comprehensive conceptual understanding and establishes a strong foundation for future empirical investigations.

The findings generated through this methodology are expected to provide actionable insights for enterprise architects, AI practitioners, cybersecurity professionals, policymakers, compliance officers, and organizational leaders seeking to implement secure, transparent, and continuously compliant Agentic AI systems within enterprise environments. The methodology ensures that conclusions are grounded in credible evidence while contributing to the expanding body of knowledge on intelligent enterprise architecture and autonomous governance.

The emergence of agentic AI-driven enterprise architecture represents a significant evolution in digital enterprise systems, where autonomous software agents, powered by advanced artificial intelligence, coordinate, reason, and execute business decisions with minimal human intervention. Unlike traditional AI systems that function as isolated predictive or analytical tools, agentic AI systems operate as goal-driven entities capable of perceiving context, planning actions, interacting with enterprise systems, and continuously learning from outcomes. When embedded within enterprise architecture, these agents transform static workflows into dynamic, self-optimizing ecosystems that enhance decision-making speed, accuracy, and resilience.

A key finding in this domain is that enterprise architecture is shifting from layered, service-oriented models toward intelligent, multi-agent ecosystems integrated across cloud-native infrastructures. Platforms such as Amazon Web Services, Microsoft, and Google increasingly provide foundational capabilities such as model hosting, agent orchestration frameworks, and event-driven compute services that support autonomous decision pipelines. These infrastructures enable agentic systems to process streaming data, invoke APIs, and execute business logic in real time, forming the backbone of autonomous enterprises.

In financial governance, agentic AI architectures enable continuous compliance through embedded monitoring agents that autonomously validate transactions, detect anomalies, and enforce regulatory rules. Instead of periodic audits, compliance becomes a continuous computational process. For instance, financial agents can monitor ERP systems, flag suspicious transactions, and automatically trigger corrective workflows. This significantly reduces compliance latency and minimizes human error. Platforms such as SAP and Oracle are increasingly integrating AI-driven governance layers into enterprise resource planning systems, allowing financial controls to operate in real time.

IV. RESULTS AND DISCUSSION

In supply chain ecosystems, agentic AI enhances resilience by enabling autonomous coordination across procurement, logistics, and distribution networks. Agents continuously evaluate disruptions such as supplier delays, geopolitical risks, or transportation bottlenecks and dynamically reroute supply flows. The integration of data platforms like Snowflake and Databricks allows these agents to access unified data lakes and perform real-time predictive analytics. This leads to improved demand forecasting, inventory optimization, and reduced operational disruptions. Agent collaboration frameworks further enable multi-agent negotiation between suppliers and logistics systems, creating self-balancing supply chains.

A critical component of this architecture is the orchestration layer, where platforms such as ServiceNow and Salesforce act as workflow intelligence hubs. These systems integrate agentic decision outputs into enterprise processes, ensuring that autonomous decisions translate into executable business actions. ServiceNow's workflow automation capabilities allow agents to trigger IT operations, compliance checks, and financial approvals, while Salesforce enhances customer-facing intelligence by enabling autonomous customer interaction management and revenue optimization.

Cloud-native infrastructure providers such as IBM, Alibaba Cloud, and Oracle support hybrid and distributed deployment of agentic systems. These platforms ensure scalability, security, and regulatory compliance across jurisdictions. Kubernetes-based orchestration environments, often deployed via platforms like Red Hat OpenShift and

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 1, January-February 2026 |

DOI:10.15662/IJEETR.2026.0801023

VMware Tanzu, enable containerized agent deployment, allowing enterprises to scale autonomous workloads dynamically while maintaining observability and policy enforcement.

A major architectural shift observed is the integration of policy-as-code and compliance-as-code frameworks within agentic systems. Instead of relying on human interpretation of regulatory requirements, rules are encoded into machine-readable policies that agents enforce autonomously. This enables continuous compliance, where every transaction, workflow, or decision is validated in real time against regulatory constraints. This reduces compliance costs while increasing auditability and transparency. However, it also introduces challenges related to explainability and trust, as organizations must ensure that autonomous decisions remain interpretable and verifiable.

Security remains a foundational concern in agentic AI-driven architectures. Autonomous agents introduce expanded attack surfaces, requiring advanced identity and access management, zero-trust architectures, and continuous monitoring. AI agents must be authenticated, authorized, and audited at every interaction point. Furthermore, adversarial risks such as data poisoning, model manipulation, and prompt injection attacks must be mitigated through robust cybersecurity frameworks. Enterprises are increasingly adopting AI governance layers that include runtime monitoring, anomaly detection, and automated rollback mechanisms.

Another important observation is that agentic systems fundamentally shift enterprise decision-making from human-centric to hybrid human-AI governance models. While agents handle operational decisions, humans increasingly assume supervisory roles focused on strategy, ethics, and exception handling. This leads to a new organizational paradigm where decision velocity increases significantly, but accountability structures must be redefined to ensure responsible AI deployment.

Overall, the results indicate that agentic AI-driven enterprise architectures represent a transformative leap in enterprise computing. They enable continuous, autonomous, and intelligent decision-making across financial governance, supply chains, and operational systems. However, their success depends on robust integration of governance, security, and explainability mechanisms that ensure trust and compliance in highly autonomous environments.

V. CONCLUSION

The study of agentic AI-driven enterprise architecture demonstrates a fundamental transformation in how modern enterprises are designed, operated, and governed. By integrating autonomous AI agents into cloud-native and data-driven infrastructures, organizations are moving toward systems capable of continuous decision-making, self-optimization, and real-time compliance enforcement. This represents a departure from traditional enterprise architectures that rely heavily on human-driven workflows and periodic decision cycles.

In financial governance, agentic AI introduces a paradigm of continuous compliance, where autonomous agents monitor, validate, and enforce regulatory requirements in real time. This reduces reliance on manual audits and improves the accuracy and timeliness of financial reporting. Platforms such as SAP and Oracle provide the structural backbone for embedding these capabilities directly into enterprise resource planning systems, ensuring that governance becomes an integral part of every financial transaction.

In supply chain management, agentic AI enhances resilience by enabling adaptive, self-correcting logistics networks. Autonomous agents can detect disruptions, evaluate alternatives, and execute corrective actions without human intervention. This improves supply chain responsiveness and reduces operational downtime. The integration of unified data platforms such as Snowflake and Databricks further strengthens these systems by providing real-time visibility and predictive intelligence.

Real-time business operations are significantly improved through agent-driven orchestration layers provided by platforms like ServiceNow and Salesforce. These systems ensure that autonomous decisions are translated into executable workflows across IT, customer service, and business operations. This leads to increased operational efficiency and improved customer experience.

Despite these advantages, the adoption of agentic AI architectures introduces challenges related to security, transparency, and governance. Autonomous systems must be carefully monitored to prevent unintended consequences, biases, and security vulnerabilities. Organizations must implement robust AI governance frameworks, including explainability mechanisms and compliance verification systems.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 1, January-February 2026 |

DOI:10.15662/IJEETR.2026.0801023

Overall, agentic AI-driven enterprise architecture represents the next stage of digital transformation. It enables enterprises to transition from reactive systems to proactive and autonomous ecosystems. However, achieving sustainable success requires balancing automation with accountability, ensuring that human oversight remains central to strategic decision-making while allowing AI agents to manage operational complexity.

VI. FUTURE WORK

Future research in agentic AI-driven enterprise architecture should focus on enhancing autonomy, interoperability, and trustworthiness of AI agents in enterprise ecosystems. One key direction is the development of standardized multi-agent communication protocols that allow agents from different vendors and platforms to collaborate seamlessly. Currently, most enterprise AI systems operate in isolated environments, limiting their ability to coordinate across organizational boundaries. Establishing open standards for agent communication and reasoning will be critical for enabling fully integrated autonomous enterprises.

Another important area is the advancement of explainable agentic AI systems. As autonomous agents take on increasingly critical decision-making roles, ensuring transparency in their reasoning processes becomes essential. Future systems must provide human-interpretable explanations for decisions, particularly in high-stakes domains such as financial governance and supply chain management. Research into explainable AI (XAI) and traceable decision logs will play a central role in building trust in these systems.

Security and resilience of agentic systems also require further exploration. As AI agents gain access to sensitive enterprise systems, they become potential targets for adversarial attacks. Future architectures must incorporate self-defending mechanisms, including real-time threat detection, autonomous patching, and adaptive access control. Zero-trust principles must be extended to AI agents themselves, ensuring that every action is continuously validated.

Edge AI integration represents another promising direction. Deploying agentic systems closer to data sources, such as IoT devices and edge nodes, will reduce latency and improve responsiveness in real-time operations. This is particularly important for industries such as manufacturing, logistics, and energy systems, where milliseconds can significantly impact outcomes.

Finally, ethical governance and regulatory alignment will be essential for future development. As autonomous decision-making becomes more prevalent, regulatory frameworks must evolve to address accountability, liability, and fairness in AI-driven decisions. Future enterprise architectures should incorporate built-in compliance with global regulatory standards and ethical AI guidelines, ensuring responsible deployment of autonomous systems at scale.

REEFERENCES

1. Amazon Web Services. (2024). AWS generative AI and agent frameworks. https://aws.amazon.com
2. Bubeck, S., et al. (2023). Sparks of artificial general intelligence: Early experiments with GPT-4. arXiv preprint.
3. Ayyagari, V. (2025). Model Context Protocol for Agentic AI: Enabling Contextual Interoperability Across Systems. Int. J. Comput. Exp. Sci. Eng, 11, 6072-6082.
4. Yatam, S. N. K. (2025). Secure and Scalable Messaging Ecosystems: Automating Multi-Platform Architectures with Adaptive Security in Multi-Cloud Environments. Journal Of Multidisciplinary, 5(7), 134-142.
5. Veershetty, G. (2023). SAP S/4HANA Transformation in the Electric Power and Grid Utility Sector: Combination Migration Strategy and Customer-Managed Deployment A Practitioner's Analysis. International Journal of Emerging Research in Engineering and Technology, 4(1), 218-227.
6. Gopisetty, S. (2025). The Auditor's Apprentice: Can a Language Model Learn to Translate AWS's Automated SAP Changes into Human-Friendly Compliance Stories?. European Journal of Advances in Engineering and Technology, 12(1), 43-50.
7. Polamreddy, V. R. (2025). Architecting Financially Compliant Enterprise Point-of-Sale Systems: Data Integrity and Revenue Recognition at Scale. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(5), 12993-13104.
8. Kaushik, K., Bharti, P., Makkena, B., Narooka, P., & Soni, M. (2025, October). Data-Driven Motion Planning for Autonomous Robots Using Deep Reinforcement Learning in Dynamic Environments. In 2025 1st IEEE Uttar Pradesh Section Women in Engineering International Conference on Electrical Electronics and Computer Engineering (UPWIECON) (pp. 180-186). IEEE.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 1, January-February 2026 |

DOI:10.15662/IJEETR.2026.0801023

9. 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
10. Gollapudi, R. (2025). Data-Driven Risk Scoring For Grid Assets Using Centralized Production Databases. International Journal Of Advances In Signal And Image Sciences, 50-87.
11. Kotla, M. R. T. (2025). Enterprise integration lessons from four digital frontlines: A comparative analysis of modern IT ecosystems. International Journal of Research Publications in Engineering, Technology and Management, 8(3), 32–42.
12. Kavuri, S. (2023). Machine learning approaches for security vulnerability detection in software testing. Computer Fraud & Security, 21-31.
13. Parasa, M. (2025). Creating hyper-personalized learning journeys using AI in SAP SuccessFactors LMS for individual development and business alignment. International Research Journal of Engineering & Applied Sciences, 13(4), 241–255. https://doi.org/10.55083/irjeas.2025.v13i04022
14. Anbalagan, B., Joyce, S., Mani, R., Bussu, V. R. R., Komarina, G. B., Mane, V., & Doshi, A. (2025, October). Accelerating SAP HANA Performance with Azure NetApp Files. In 2025 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1-6). IEEE.
15. Google. (2024). Vertex AI and agent development framework. https://cloud.google.com
16. Goel, N. (2023). Zero Trust Architecture: A Revolutionary Approach to Cybersecurity. Res Militaris, Volume 13, Issue 3, pp. 6931–6940.
17. Lanka, S. (2025). AI driven healthcare at scale: Personalization and predictive tools in the CVS Health mobile app. International Journal of Research and Applied Innovations, 8(3), 12280-12297.
18. Anumula, S. K. (2025). Design-Based Supply Chain Operations Research Model: Fostering Resilience And Sustainability In Modern Supply Chains. arXiv preprint arXiv:2511.01878.
19. Microsoft. (2024). Autonomous agents in Azure AI. https://learn.microsoft.com
20. Oracle. (2023). AI-driven enterprise applications. https://www.oracle.com
21. SAP. (2023). Business AI and intelligent enterprise architecture. https://www.sap.com
22. Rajan, P. K. (2023). Predictive Caching in Mobile Streaming Applications using Machine Learning Models. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(3), 8737-8745.
23. ServiceNow. (2023). AI-driven workflow automation. https://www.servicenow.com
24. Weber, J., & Hauer, M. (2021). Autonomous systems in enterprise architecture. Journal of Cloud Computing, 10(2), 1–18.
25. Syed, S. (2025). Enterprise asset management digitalization for multi-site pharmaceutical manufacturing: A transatlantic Oracle eAM implementation. International Journal of Computer Technology and Electronics Communication (IJCTEC), 8(4), 11138–11146. https://doi.org/10.15680/IJCTECE.2025.0804018
26. Barigidad, S., Hameed, S., Karri, N., Jangam, S. K., Pedda, P. S. R., & Gupta, D. (2025, December). Computational Modeling of AI-Enhanced Learning Pathways: A Mathematical Framework for Optimizing Knowledge Acquisition, Cognitive Load Management, and Student Performance in STEM Education. In 2025 International Conference on AI-Driven STEM Education and Learning Technologies (AISTEMEDU) (pp. 1-7). IEEE.
27. Sivakumer, D. (2023). ServiceNow-based project management models for scalable enterprise workflow automation. International Journal of Future Innovative Science and Technology (IJFIST), 6(4), 11003–11014. https://doi.org/10.15662/IJFIST.2023.0604006
28. Sarngadharan, S. (2025). Self-optimizing pipelines: ML systems that tune themselves in production. International Journal of Computer Technology and Electronics Communication (IJCTEC), 8(2), 10468–10476. https://doi.org/10.15680/IJCTECE.2025.0802015
29. Damarched, M. K. (2025). Data Governance Challenges in ITSM Platform Transitions. International Journal of Computer Technology and Electronics Communication, 8(6), 11881-11890.
30. Singh, A. (2025). AI-driven autonomous network control planes for large-scale infrastructure networks. International Journal of Computer Technology and Electronics Communication, 8(6), 11705-11715.
31. Govindan, V. (2025). Vendor dependency to enterprise sovereignty: A phased migration approach for enterprise applications. International Journal of Computer Technology and Electronics Communication (IJCTEC), 8(4), 11176–11185. https://doi.org/10.15680/IJCTECE.2025.0804021
32. Upadhyay, H. (2025). Consumer Experience Trends Based on AI Features: A Comprehensive Analysis of Conversational AI, Personalization Engines, and Voice AI. Frontiers in Emerging Artificial Intelligence and Machine Learning, 2(11), 6-15.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 1, January-February 2026 |

DOI:10.15662/IJEETR.2026.0801023

33. 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.
34. Rongali, L. P. (2025). Compliance and Governance: Address the Role of Devops in Maintaining Compliance and Ensuring Governance throughout the Development Lifecycle. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5229546
35. 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.
36. Chenna, S. (2025). Modernizing enterprise integration architecture: A case study of Oracle Cloud Integration. International Journal of Computer Technology and Electronics Communication, 8(3), 10768–10775. https://doi.org/10.15680/IJCTECE.2025.0803012
37. Gandikota, S. P. (2025). High-availability network diagnostics and configuration platform for real-time financial service delivery. International Journal of Computer Technology and Electronics Communication (IJCTEC), 8(4), 11147–11160. https://doi.org/10.15680/IJCTECE.2025.0804019
38. Mannem, S. (2025). Automated patient quality data flow for CMS reporting accuracy. International Journal of Computer Technology and Electronics Communication (IJCTEC), 8(4), 11161–11175. https://doi.org/10.15680/IJCTECE.2025.0804020
39. Chettiyar, S. S. S. (2025). Agentic orchestration and integration of PBX and SaaS CRM platforms. International Journal of Computer Technology and Electronics Communication (IJCTEC), 8(2), 10451–10467. https://doi.org/10.15680/IJCTECE.2025.0802014
40. Zhang, Y., et al. (2022). Multi-agent reinforcement learning in enterprise systems. IEEE Transactions on Systems, Man, and Cybernetics.