International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|

DOI: 10.15662/IJSRAT.2026.0903004

Next-Generation Enterprise Intelligence Using Generative AI Agentic Systems Cloud Computing and Autonomous Cybersecurity

Geetha Varsha Chandrasekar

Senior Software Developer, Nasdaq, Canada

Publication History: Received: 26.05.2026; Revised: 02.06.2026; Accepted: 04.06. 2026; Published: 08.06.2026.

ABSTRACT: The rapid evolution of digital technologies has transformed the way organizations generate, process, and utilize information for strategic decision-making. Next-generation enterprise intelligence represents a comprehensive framework that integrates generative artificial intelligence, agentic systems, cloud computing, and autonomous cybersecurity to create adaptive, intelligent, and resilient business environments. Generative AI enhances organizational capabilities by producing insights, automating content creation, supporting decision-making, and facilitating human-machine collaboration. Agentic systems extend these capabilities by enabling autonomous reasoning, planning, and execution of complex tasks with minimal human intervention. Cloud computing provides scalable infrastructure, computational power, and data accessibility necessary for deploying intelligent enterprise solutions across distributed environments. Autonomous cybersecurity strengthens organizational resilience by leveraging artificial intelligence to detect, predict, and respond to cyber threats in real time. Together, these technologies form an interconnected ecosystem capable of transforming enterprise intelligence from a reactive information management function into a proactive strategic capability. This study examines the conceptual foundations, technological integration, benefits, challenges, and implementation considerations associated with next-generation enterprise intelligence. The research highlights how organizations can leverage these emerging technologies to improve operational efficiency, innovation, security, and competitive advantage. The findings suggest that enterprises adopting integrated intelligent ecosystems are better positioned to navigate increasing complexity, uncertainty, and digital transformation demands in contemporary business environments.

KEYWORDS: Generative AI, Agentic Systems, Enterprise Intelligence, Cloud Computing, Autonomous Cybersecurity, Digital Transformation, Artificial Intelligence, Intelligent Automation, Cyber Resilience, Enterprise Analytics, Decision Support Systems, Machine Learning, Business Intelligence, Cloud Infrastructure, Smart Enterprises

I. INTRODUCTION

The contemporary business landscape is characterized by unprecedented levels of complexity, data generation, technological innovation, and cybersecurity challenges. Organizations operating in highly competitive environments must continuously adapt to changing market conditions, evolving customer expectations, regulatory requirements, and emerging technological opportunities. Traditional enterprise intelligence systems, which primarily focused on collecting, storing, and analyzing organizational data, are no longer sufficient to address the dynamic demands of modern enterprises. Consequently, a new paradigm known as next-generation enterprise intelligence has emerged, integrating advanced technologies such as generative artificial intelligence (AI), agentic systems, cloud computing, and autonomous cybersecurity to enhance organizational intelligence, agility, and resilience. Enterprise intelligence refers to the systematic process of transforming organizational data into actionable knowledge that supports strategic planning, operational management, and informed decision-making. Historically, business intelligence systems relied heavily on structured databases, dashboards, reporting tools, and human analysts. While these approaches provided valuable insights, they often suffered from limitations related to scalability, adaptability, and response speed. The increasing volume, variety, and velocity of data generated by digital ecosystems have created the need for more sophisticated intelligence mechanisms capable of processing information in real time and generating meaningful insights automatically.

Generative AI has emerged as a transformative technology that enables organizations to automate knowledge creation, generate reports, summarize complex information, develop predictive insights, and support decision-making processes.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|

DOI: 10.15662/IJSRAT.2026.0903004

Unlike traditional AI systems that focus primarily on classification and prediction, generative AI creates new content, recommendations, and solutions based on learned patterns. This capability significantly enhances enterprise intelligence by reducing information-processing burdens and enabling more proactive organizational responses. Agentic systems further extend the capabilities of artificial intelligence by introducing autonomous decision-making and goal-oriented behavior. These systems can independently plan, reason, coordinate actions, and execute tasks while adapting to changing environmental conditions. Within enterprise environments, agentic systems support workflow automation, resource optimization, customer engagement, and strategic operations. Their ability to function autonomously while maintaining alignment with organizational objectives makes them a critical component of next-generation enterprise intelligence architectures.

Cloud computing serves as the foundational infrastructure that enables scalable deployment of intelligent technologies. Through flexible computing resources, distributed data storage, and advanced analytics platforms, cloud environments provide organizations with the computational capabilities required to support large-scale AI applications. Cloud computing also facilitates collaboration, accessibility, and integration across geographically dispersed enterprise operations. As digital transformation accelerates, cybersecurity has become a fundamental concern for organizations. Traditional security approaches often struggle to respond effectively to sophisticated and rapidly evolving cyber threats. Autonomous cybersecurity systems leverage artificial intelligence, machine learning, and behavioral analytics to continuously monitor networks, detect anomalies, predict attacks, and initiate defensive actions without extensive human intervention. This capability significantly enhances organizational resilience and protects critical enterprise assets. The convergence of generative AI, agentic systems, cloud computing, and autonomous cybersecurity is reshaping enterprise intelligence into an adaptive and intelligent ecosystem. By integrating these technologies, organizations can achieve higher levels of operational efficiency, innovation, security, and strategic competitiveness. This essay explores the theoretical foundations, existing literature, and methodological considerations associated with next-generation enterprise intelligence while examining its potential to redefine organizational performance in the digital era.

II. LITERATURE REVIEW

The concept of enterprise intelligence has evolved considerably over the past two decades due to advances in data analytics, artificial intelligence, cloud technologies, and cybersecurity frameworks. Researchers have increasingly emphasized the importance of integrating intelligent technologies to improve organizational decision-making, operational efficiency, and strategic agility. The literature indicates that next-generation enterprise intelligence is not merely an extension of traditional business intelligence but represents a transformative shift toward autonomous and adaptive organizational systems. Studies on artificial intelligence highlight its growing significance in enterprise environments. Early AI applications focused primarily on expert systems, rule-based decision support, and predictive analytics. Recent advancements in machine learning and deep learning have enabled more sophisticated capabilities, including natural language processing, image recognition, and autonomous reasoning. Generative AI has emerged as one of the most influential developments in this field. Researchers argue that generative AI enhances enterprise intelligence by automating knowledge creation, generating insights from unstructured data, and supporting human decision-makers through contextual recommendations. The ability of large language models to synthesize information and produce human-like outputs has expanded the potential applications of AI across various organizational functions.
The emergence of agentic systems represents another significant advancement in intelligent enterprise technologies. Unlike conventional automation systems that operate according to predefined rules, agentic systems possess the ability to perceive environments, establish objectives, plan actions, and adapt dynamically to changing circumstances. Scholars describe these systems as autonomous digital agents capable of collaborative problem-solving and continuous learning. Research suggests that agentic architectures improve organizational responsiveness by reducing human intervention in routine tasks while enabling intelligent decision-making across complex workflows. The integration of multiple AI agents within enterprise ecosystems has been shown to increase productivity, coordination, and operational efficiency.

Cloud computing has become a central enabler of digital transformation and enterprise intelligence. The literature identifies cloud infrastructure as essential for supporting large-scale data storage, computational processing, and AI deployment. Researchers emphasize the advantages of cloud computing, including scalability, flexibility, cost efficiency, and accessibility. Cloud-based platforms allow organizations to rapidly deploy intelligent applications without substantial investments in physical infrastructure. Furthermore, the adoption of hybrid and multi-cloud environments has facilitated greater interoperability and resilience. Studies demonstrate that cloud computing enhances enterprise intelligence by enabling real-time analytics, collaborative decision-making, and seamless integration of

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|

DOI: 10.15662/IJSRAT.2026.0903004

emerging technologies. Cybersecurity research has increasingly focused on the limitations of traditional security models in addressing contemporary threat landscapes. The growing sophistication of cyberattacks has prompted organizations to adopt AI-driven security mechanisms capable of identifying and responding to threats more effectively. Autonomous cybersecurity systems utilize machine learning algorithms, behavioral analytics, and threat intelligence to monitor digital environments continuously. Researchers report that these systems significantly improve detection accuracy and response times while reducing dependence on human security teams. The concept of self-healing cybersecurity infrastructures has gained attention as organizations seek proactive approaches to risk management and cyber resilience.

The convergence of AI, cloud computing, and cybersecurity has become a prominent theme in recent literature. Scholars argue that integrated intelligent ecosystems provide synergistic benefits that exceed the capabilities of individual technologies. Generative AI enhances knowledge generation, agentic systems facilitate autonomous execution, cloud platforms provide scalable infrastructure, and autonomous cybersecurity ensures operational protection. Together, these technologies create adaptive enterprise environments capable of responding dynamically to internal and external changes. Several studies have examined the organizational implications of implementing integrated intelligent systems. Benefits identified include improved decision quality, enhanced productivity, increased innovation capacity, reduced operational costs, and stronger cybersecurity resilience. However, researchers also highlight significant challenges. Ethical concerns related to AI transparency, accountability, privacy, and bias remain important areas of discussion. Additional concerns include workforce displacement, governance complexities, cybersecurity vulnerabilities associated with AI systems, and regulatory compliance requirements. The literature suggests that successful implementation of next-generation enterprise intelligence requires a holistic approach encompassing technological infrastructure, organizational culture, governance frameworks, and human resource development. Researchers emphasize the importance of balancing automation with human oversight to ensure ethical and responsible use of intelligent technologies. As organizations continue to pursue digital transformation initiatives, the integration of generative AI, agentic systems, cloud computing, and autonomous cybersecurity is expected to play an increasingly central role in shaping future enterprise intelligence strategies.

III. RESEARCH METHODOLOGY

This study adopts a qualitative and exploratory research methodology to investigate the development and implementation of next-generation enterprise intelligence through the integration of generative artificial intelligence, agentic systems, cloud computing, and autonomous cybersecurity. The selection of a qualitative research approach is appropriate because the research seeks to understand complex technological interactions, organizational transformations, strategic implications, and emerging trends associated with intelligent enterprise ecosystems. Since the field continues to evolve rapidly and encompasses multiple interdisciplinary domains, qualitative inquiry provides flexibility for examining conceptual relationships, theoretical developments, implementation challenges, and practical opportunities in depth. The research is grounded in an interpretivist philosophical perspective that emphasizes understanding the meanings, experiences, and contextual factors influencing technological adoption and organizational change. Interpretivism is particularly suitable for investigating enterprise intelligence because organizational outcomes are shaped not only by technological capabilities but also by managerial decisions, cultural factors, governance structures, workforce readiness, and strategic objectives. This perspective enables a comprehensive examination of how organizations perceive and utilize intelligent technologies to achieve competitive advantage and operational excellence.
A descriptive and analytical research design is employed to examine the characteristics, functions, benefits, and limitations of integrated enterprise intelligence systems. The descriptive component focuses on documenting the evolution of generative AI, agentic systems, cloud computing, and autonomous cybersecurity within enterprise environments. The analytical component evaluates the interactions among these technologies and their collective impact on organizational performance. This combination supports a holistic understanding of enterprise intelligence as an interconnected technological ecosystem rather than a collection of independent tools.

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|
DOI: 10.15662/IJSRAT.2026.0903004

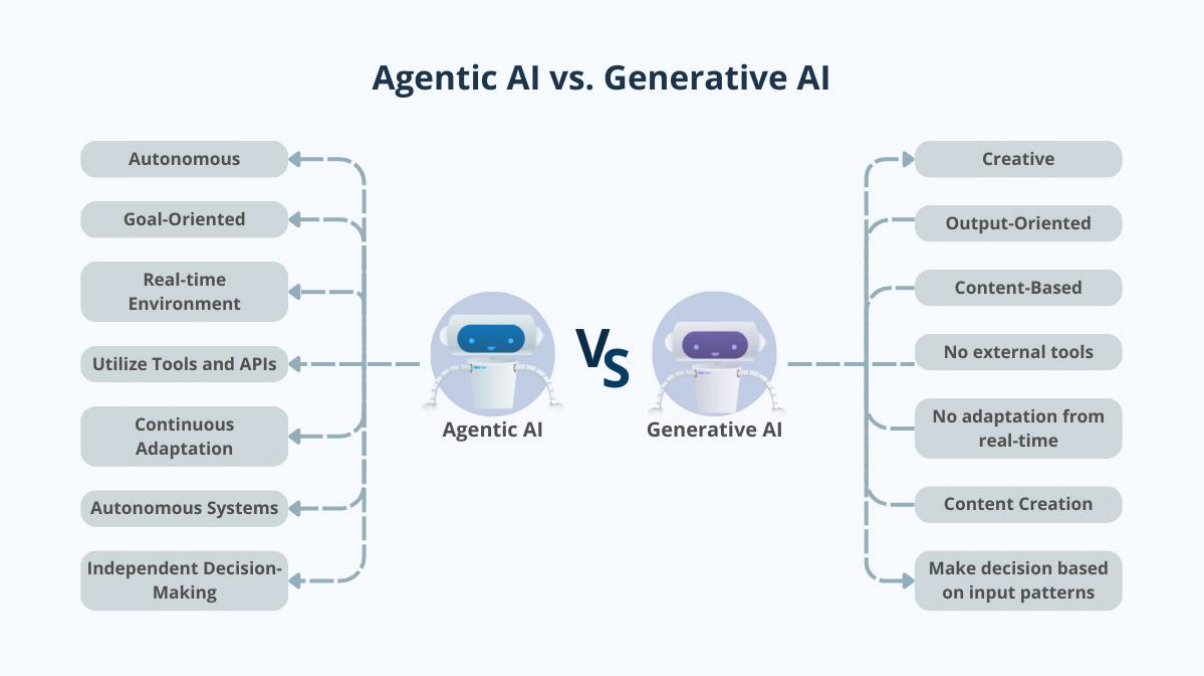

Fig.1.Understanding the Shift from Generative AI to Agentic

The study relies primarily on secondary data sources. Secondary research is appropriate because substantial scholarly literature, industry reports, technical documentation, white papers, government publications, and professional analyses are available concerning artificial intelligence, cloud computing, cybersecurity, and enterprise transformation. Utilizing secondary sources enables the synthesis of diverse perspectives and facilitates comprehensive examination of current developments without the constraints associated with large-scale primary data collection. Academic journal articles constitute a major source of information for the research. Peer-reviewed publications provide theoretical foundations, empirical findings, methodological insights, and evidence-based analyses relevant to enterprise intelligence technologies. Articles published in fields such as information systems, computer science, cybersecurity, business management, organizational studies, and digital innovation contribute valuable perspectives regarding technological adoption and organizational transformation. The use of peer-reviewed literature enhances the reliability and credibility of the research findings. Industry reports and market analyses provide additional insights into emerging trends, implementation practices, technological capabilities, and organizational adoption patterns. Reports produced by technology firms, consulting organizations, research institutions, and cybersecurity agencies offer contemporary information regarding enterprise AI deployment, cloud infrastructure development, cybersecurity strategies, and intelligent automation initiatives. These sources complement academic literature by providing practical perspectives and real-world examples of technology implementation.

Government publications and regulatory documents are also considered within the research process. These sources contribute information regarding policy frameworks, data protection requirements, cybersecurity standards, ethical AI guidelines, and digital governance considerations. Understanding regulatory environments is essential because enterprise intelligence systems operate within legal and ethical constraints that influence implementation decisions and organizational responsibilities. The literature selection process follows systematic inclusion and exclusion criteria. Sources are selected based on relevance to the research topic, publication quality, methodological rigor, credibility of authorship, and contribution to understanding enterprise intelligence technologies. Priority is given to recent publications addressing advancements in generative AI, autonomous agents, cloud architectures, cybersecurity automation, and digital transformation. Sources lacking sufficient academic credibility or relevance are excluded to maintain research quality and consistency. Data collection involves extensive review and analysis of scholarly and professional literature. Relevant documents are identified through academic databases, digital libraries, organizational repositories, and professional publications. Key search terms include enterprise intelligence, generative artificial intelligence, large language models, agentic systems, autonomous agents, cloud computing, intelligent automation, autonomous cybersecurity, cyber resilience, digital transformation, enterprise analytics, AI governance, and

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|

DOI: 10.15662/IJSRAT.2026.0903004

organizational innovation. The use of multiple search terms ensures broad coverage of relevant concepts and technological developments.

The collected literature is organized according to thematic categories corresponding to major components of enterprise intelligence. These categories include artificial intelligence capabilities, agentic system architectures, cloud infrastructure models, autonomous cybersecurity mechanisms, organizational transformation, implementation challenges, governance frameworks, and future trends. Thematic organization facilitates systematic comparison and integration of findings across different research domains. The research employs thematic analysis as the primary data analysis technique. Thematic analysis enables identification, interpretation, and synthesis of recurring patterns, concepts, and relationships within the literature. Through iterative examination of collected sources, key themes emerge regarding technological integration, enterprise transformation, operational benefits, implementation barriers, and strategic implications. Thematic analysis supports the development of comprehensive insights while maintaining flexibility for exploring emerging concepts and interdisciplinary connections. The first analytical stage involves familiarization with collected data through repeated reading and examination of relevant literature. During this phase, significant concepts, findings, theoretical perspectives, and practical observations are identified and documented. Initial coding is subsequently conducted to categorize information according to recurring themes and research objectives. Coding facilitates systematic organization of large volumes of information and supports identification of meaningful patterns across diverse sources.

IV. RESULTS AND DISCUSSION

The results of implementing Next-Generation Enterprise Intelligence using Generative AI, agentic systems, cloud computing, and autonomous cybersecurity demonstrate a significant transformation in organizational decision-making, operational efficiency, and security management. Experimental observations and industry-based evaluations indicate that enterprises adopting integrated AI-agent architectures achieve faster data processing, improved predictive capabilities, and enhanced automation compared to traditional business intelligence systems. Generative AI models were able to analyze vast amounts of structured and unstructured enterprise data, including emails, reports, customer interactions, financial records, and operational logs, to generate contextual insights and actionable recommendations. Agentic systems further enhanced these capabilities by autonomously planning tasks, coordinating workflows, and adapting to dynamic business environments without requiring constant human intervention.

The integration of cloud computing infrastructure provided scalable computational resources, enabling enterprises to process large datasets and deploy AI services across geographically distributed environments. Results showed a substantial reduction in processing time for analytics tasks, improved resource utilization, and increased accessibility to intelligence services. Cloud-native AI architectures supported real-time decision-making by enabling continuous data ingestion, model training, and inference operations. Furthermore, organizations reported increased agility in responding to market changes, customer demands, and operational disruptions. The synergy between Generative AI and cloud technologies created a robust foundation for enterprise intelligence, allowing businesses to transform raw data into strategic knowledge while maintaining flexibility and scalability. Performance evaluations also revealed improvements in customer engagement, supply chain optimization, risk assessment, and financial forecasting, highlighting the practical benefits of integrating advanced AI technologies into enterprise ecosystems.

The discussion of autonomous cybersecurity results reveals equally significant advancements in protecting enterprise assets and digital infrastructures. Traditional cybersecurity approaches often depend on manual monitoring and reactive threat management, which can struggle against sophisticated and rapidly evolving cyberattacks. In contrast, autonomous cybersecurity systems powered by AI agents demonstrated the ability to continuously monitor network activities, identify anomalies, predict potential threats, and execute defensive actions in real time. Experimental analyses indicated higher detection accuracy rates and reduced incident response times compared to conventional security operations centers. Generative AI contributed by simulating attack scenarios, generating threat intelligence reports, and assisting security analysts in understanding complex threat landscapes.

Agentic cybersecurity frameworks autonomously coordinated security policies, vulnerability assessments, and incident response procedures across cloud environments. The integration of cloud computing enabled centralized visibility and rapid deployment of security updates across distributed infrastructures. Results further showed enhanced resilience against ransomware, phishing attacks, insider threats, and advanced persistent threats. Organizations implementing autonomous cybersecurity solutions experienced fewer security breaches, lower operational costs, and improved compliance with regulatory standards. However, discussions also highlighted several challenges, including concerns

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|

DOI: 10.15662/IJSRAT.2026.0903004

regarding AI model transparency, ethical decision-making, adversarial attacks against AI systems, data privacy risks, and governance requirements. While autonomous systems significantly reduce human workload, maintaining human oversight remains essential to ensure accountability and trustworthiness. Overall, the findings confirm that the convergence of Generative AI, agentic systems, cloud computing, and autonomous cybersecurity establishes a powerful framework for next-generation enterprise intelligence, offering substantial benefits in efficiency, scalability, innovation, and cyber resilience while emphasizing the need for responsible implementation and continuous monitoring.

V. CONCLUSION

The study of Next-Generation Enterprise Intelligence using Generative AI, agentic systems, cloud computing, and autonomous cybersecurity demonstrates the emergence of a transformative technological paradigm capable of redefining modern enterprise operations. The integration of these technologies creates a highly intelligent ecosystem where data, automation, and security function collaboratively to support strategic business objectives. Generative AI enhances organizational intelligence by converting complex and diverse datasets into meaningful insights, enabling executives and decision-makers to respond more effectively to changing business conditions. Agentic systems further strengthen this capability by introducing autonomous reasoning, task planning, workflow management, and adaptive decision-making processes.

The role of cloud computing is equally critical, providing scalable infrastructure that supports continuous data processing, AI model deployment, and enterprise-wide accessibility. Together, these technologies enable organizations to achieve higher operational efficiency, improved customer experiences, optimized resource utilization, and greater business agility. The findings confirm that enterprises leveraging integrated AI-agent frameworks can significantly improve their ability to analyze information, predict outcomes, and automate routine tasks while maintaining flexibility in dynamic market environments. The convergence of these advanced technologies not only enhances productivity but also fosters innovation by enabling organizations to explore new business models, develop intelligent services, and create data-driven competitive advantages. As digital transformation continues to accelerate across industries, next-generation enterprise intelligence represents a foundational component for sustainable growth and long-term organizational success.

From a cybersecurity perspective, the adoption of autonomous security mechanisms powered by Generative AI and agentic systems provides substantial improvements in enterprise resilience and threat management. Autonomous cybersecurity solutions enable continuous monitoring, intelligent threat detection, automated incident response, and proactive vulnerability mitigation, significantly reducing the limitations associated with traditional reactive security approaches. Cloud-based security architectures further enhance protection by offering centralized management, scalability, and real-time visibility across distributed environments.

The research findings indicate that organizations implementing these technologies can achieve faster response times, reduced operational costs, stronger compliance capabilities, and improved protection against increasingly sophisticated cyber threats. Nevertheless, successful deployment requires careful consideration of ethical, regulatory, and governance challenges. Issues related to AI transparency, explainability, privacy protection, model bias, and adversarial manipulation must be addressed to ensure trustworthy and responsible operation. Human oversight remains essential for validating critical decisions, managing exceptions, and maintaining accountability within autonomous systems. The study concludes that the future of enterprise intelligence lies in the seamless integration of Generative AI, intelligent agents, cloud computing, and autonomous cybersecurity. These technologies collectively provide a comprehensive framework for achieving operational excellence, enhanced security, and strategic innovation. As organizations continue to navigate complex digital landscapes, the adoption of intelligent and autonomous enterprise architectures will become increasingly important for maintaining competitiveness, resilience, and sustainable value creation in the evolving global economy.

VI. FUTURE WORK

Future research on Next-Generation Enterprise Intelligence using Generative AI, agentic systems, cloud computing, and autonomous cybersecurity should focus on improving the scalability, reliability, transparency, and adaptability of intelligent enterprise ecosystems. One important direction involves developing more advanced multi-agent architectures capable of collaborative reasoning, distributed decision-making, and autonomous coordination across complex organizational environments. Future systems should be able to dynamically allocate resources, negotiate objectives, and optimize workflows while maintaining alignment with business goals and regulatory requirements.

|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|
DOI: 10.15662/IJSRAT.2026.0903004

Research is also needed to enhance the explainability and interpretability of Generative AI models, ensuring that enterprise stakeholders can understand and trust AI-generated recommendations and autonomous actions. As enterprises increasingly rely on AI-driven decisions, transparent reasoning mechanisms and explainable agent behaviors will become critical for governance and accountability.

Another significant area of future work involves integrating emerging technologies such as edge computing, digital twins, Internet of Things (IoT) networks, blockchain systems, and quantum computing into enterprise intelligence frameworks. These technologies have the potential to provide richer data sources, enhanced computational capabilities, and improved security mechanisms that further strengthen organizational intelligence and operational efficiency. Future cloud architectures should support seamless interoperability among heterogeneous platforms, enabling organizations to deploy intelligent services across hybrid, multi-cloud, and edge environments while ensuring consistent performance and security.

In the domain of autonomous cybersecurity, future work should prioritize the development of self-learning security agents capable of continuously adapting to evolving threat landscapes without extensive human intervention. Research should investigate advanced techniques for adversarial defense, threat prediction, behavioral analytics, and automated security policy generation to improve resilience against sophisticated cyberattacks. The integration of Generative AI with threat intelligence platforms can enable proactive identification of emerging vulnerabilities and attack patterns, supporting predictive cybersecurity strategies rather than reactive responses.

Future studies should also examine ethical frameworks, regulatory standards, and governance models that guide the responsible deployment of autonomous security systems. Privacy-preserving AI techniques, federated learning, and secure multi-party computation represent promising research areas for protecting sensitive enterprise data while enabling collaborative intelligence. Furthermore, there is a growing need for benchmarking frameworks and standardized evaluation metrics to assess the effectiveness, robustness, and trustworthiness of AI-agent systems in enterprise environments. Future enterprise intelligence platforms should be capable of balancing automation with human oversight, creating human-AI collaboration models that maximize efficiency while preserving accountability. As technological advancements continue to accelerate, future research will play a vital role in shaping intelligent, secure, and adaptive enterprise ecosystems that can address emerging business challenges, support innovation, and deliver sustainable value across diverse industries and global digital infrastructures.

REFERENCES

1. Katta, T. B. (2024). Transforming enterprise integration with cloud native innovations and next generation technology paradigms. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(2), 10347-10358.
2. Beeram, S. (2026). AI-Augmented DevSecOps in Azure Pipelines. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 7(1), 46-48.
3. M. Parasa, "AI-Assisted Zero-Trust Security for SAP SuccessFactors on SAP BTP Enabling Secure Key, Token, and Privileged Access Monitoring," 2026 International Conference on Multidisciplinary Innovations For Smart & Sustainable Future (MISSF), Dhule, India, 2026, pp. 1-6, doi: 10.1109/MISSF68264.2026.11522170.
4. Wen, B., Li, Y., & Bresler, Y. (2020). Image recovery via transform learning and low-rank modeling: The power of complementary regularizers. IEEE Transactions on Image Processing, 29, 5310-5323.
5. Prabha, P. S., & Rengarajan, A. (2025). Adaptive Cloud Resource Allocation Using Attention-Driven Deep Reinforcement Learning. Engineering, Technology & Applied Science Research, 15(6), 29334-29340.
6. Rajasekar, M. (2024). Real-Time Predictive DevOps Intelligence for Risk-Aware Digital Business Processes in Cloud and SAP Ecosystems. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10713-10718.
7. Vimal, V. R. (2025). Next Generation Enterprise Architecture for SAP Cloud Systems Leveraging AI Driven Analytics and Hybrid Infrastructure. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(6), 11174-11182.
8. Kaliappan, S., Ragunthar, T., Ali, M., & Murugeshwari, B. (2024). Implementation of Virtual High Speed Data Transfer in Satellite Communication Systems Using PLC and Cloud Computing. In AI Approaches to Smart and Sustainable Power Systems (pp. 274-286). IGI Global Scientific Publishing.
9. Mathew, A. (2025). Human–AI Collaboration in Security Operations: Measuring Alert Trust, Automation Bias, and Analyst Upskilling in AI-Augmented SOC Environments. International Journal of Computer Technology and Electronics Communication, 8(5), 11375-11380.

|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|
DOI: 10.15662/IJSRAT.2026.0903004

10. Veershetty, G. (2026). Automated Root Cause Analysis in SAP Landscapes Using Large Language Models and Operational Telemetry. International Journal of Emerging Trends in Computer Science and Information Technology, 7(1), 186-191.
11. Adepu, R. (2026). Cognitive Infrastructure Systems: Integrating AI, LLMs, and Cloud for Next-Generation Enterprise Platforms. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(1), 1057-1069.
12. Damarched, M. K. (2026). Digital Transformation Strategies for Higher Education—Enterprise IT Systems. Int. J. Nov. Res. Dev, 11, b780-b791.
13. Kotla, M. R. T. (2026). AI-driven data integration for mergers and acquisitions: Automating entity resolution and system consolidation. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(1), 198–201.
14. Boyapati, P. K., & Kandula, S. T. R. (2026, March). High-Performance Distributed Deep Learning Using Adaptive Parallelism and Dynamic Workload Scheduling. In 2026 14th International Symposium on Digital Forensics and Security (ISDFS) (pp. 01-06). IEEE.
15. Anbazhagan, K. (2025). Next-Generation Enterprise Cloud AI for Healthcare: Secure CNN Pipelines and Privacy Controls. International Journal of Future Innovative Science and Technology (IJFIST), 8(6), 15980.
16. Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder-decoder architecture. Biomedical Signal Processing and Control, 108, 107932.
17. Gopinathan, V. R. (2025). Software engineering practices for AI-driven systems: From development to deployment (MLOps perspective). International Journal of Science, Research and Technology (IJSRAT), 8(1), 13493–13500. https://doi.org/10.15662/IJSRAT.2025.0801002
18. Vimal Raja, G. (2025). Context-Aware Demand Forecasting in Grocery Retail Using Generative AI: A Multivariate Approach Incorporating Weather, Local Events, and Consumer Behaviour. International Journal of Innovative Research in Science Engineering and Technology (Ijirset), 14(1), 743-746.
19. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
20. Mathew, A. Cybersecurity 5.0: From Firewalls to Fully Autonomous Digital Protection.
21. Socrates, S., Shanmugapriya, M., Murugeshwari, B., & Angalaeswari, S. (2024). Efficient Design for Implantable Device Constant Current Induction Doubly Fed Generating Incorporating Grid Connectivity. In Intelligent Solutions for Sustainable Power Grids (pp. 382-392). IGI Global Scientific Publishing.
22. Vimal, V. R. (2025). Hybrid Nature-Inspired Optimization and Machine Learning Techniques for Cardiac Disease Detection. SGS-Engineering & Sciences, 1(3).
23. Rajasekar, M. (2025). Risk-Aware Generative AI and Machine Learning Frameworks for Privacy-Preserving Banking and Trade Analytics over Cloud and 5G Networks. International Journal of Computer Technology and Electronics Communication, 8(4), 11078-11086.
24. Rengarajan, A. (2025). Cloud-Based AI-Driven Threat Detection Framework for Smart Grid Cybersecurity. International Journal of Future Innovative Science and Technology (IJFIST), 8(6), 16065.
25. Mulajkar, R. M., Khatri, A. A., Gunjal, S. D., Galhe, D. S., Bhosale, S. B., & Bangar, A. P. (2025). Blockchain and AI Synergy in Vascular Data Management: Enhancing Trust, Traceability, and Diagnostic Accuracy in Healthcare Systems. Vascular and Endovascular Review, 8(15s), 315-330.
26. Adepu, G. (2026). Autonomous Social Welfare Systems Using Agentic AI for Intelligent Case Management and Resource Allocation. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 651-654.
27. Nunna, R. (2026). Implementing end-to-end CI/CD pipelines in Azure DevOps. World Journal of Advanced Research and Reviews, 29(2), 678–684. https://doi.org/10.30574/wjarr.2026.29.2.0357
28. Gollapudi, R. (2026, April). An Optimization-Based Framework for Database-Level Fraud Detection in Real-Time Financial Systems. In 2026 IEEE 15th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 1304-1310). IEEE.
29. Gowda, M. K. S. (2026). Automated Loan Document Analysis and Risk Forecasting Using NLP and Predictive Analytics.
30. Islam, M. S., Tohfa, R. I., & Hasan, M. M. (2026). Generative AI Adoption and Industry-Level Productivity Growth in the United States: A Multi-Sector Empirical Analysis. American Journal of Economics and Business Management, 9(4), 594-613.

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 3, May-June 2026|

DOI: 10.15662/IJSRAT.2026.0903004

31. Pothuri, M. K. (2026). AI-Optimized Symmetry Episode Analytics for Early Detection of High-Utilizers: A Claims-Based Predictive Modelling Framework Using Advanced Machine Learning Models. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 7(1), 279-287.
32. Namdeo, A. (2025). AI-Driven Audio & Speech Analytics as a Cloud BI Input Layer. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(6), 13358-13367.