International Journal of Recent Advances in Science and Technology, 2025; 11(4): 22-29

# Agentic AI Framework for Multi-Cloud DevSecOps Automation and Software Supply Chain Security

**Dr. G. Simi Margarat**

Professor, Department of Information Technology, Agni College of Technology, Chennai, India

**ABSTRACT**

The rapid adoption of multi-cloud environments has transformed software development and deployment practices, creating complex challenges in DevSecOps automation, security governance, and software supply chain protection. Traditional DevSecOps approaches often depend on rule-based automation, fragmented security tools, and human-driven decision-making, which limits scalability and responsiveness against emerging cyber threats. This research proposes an Agentic Artificial Intelligence (AI) framework designed to enhance multi-cloud DevSecOps automation and strengthen software supply chain security through autonomous, intelligent, and adaptive agents. The proposed framework integrates AI-driven agents capable of continuous monitoring, threat detection, policy enforcement, vulnerability management, compliance assessment, and automated remediation across heterogeneous cloud platforms.

The framework combines machine learning, large language models, security orchestration, infrastructure-as-code validation, and supply chain intelligence to create a proactive security ecosystem. Agentic AI enables autonomous reasoning, collaboration among specialized agents, and dynamic decision-making throughout the software development lifecycle. The research methodology adopts a design science research approach involving framework development, architecture modeling, and evaluation through security automation scenarios. The proposed model aims to reduce operational complexity, improve threat response time, and enhance visibility across distributed cloud environments. The study contributes an intelligent DevSecOps paradigm that supports secure, resilient, and automated software delivery pipelines.

**KEYWORDS**: Agentic AI, Multi-Cloud Computing, DevSecOps Automation, Software Supply Chain Security, Artificial Intelligence Agents, Cloud Security, Continuous Integration and Continuous Deployment, Cybersecurity Automation, Infrastructure as Code, Secure Software Development

## I. INTRODUCTION

Digital transformation has accelerated the adoption of cloud-native technologies, microservices architectures, container platforms, and continuous software delivery models. Organizations increasingly utilize multiple cloud service providers to achieve scalability, availability, cost optimization, and business flexibility. However, multi-cloud environments introduce significant operational and security challenges due to heterogeneous infrastructures, diverse security controls, complex identity management systems, and inconsistent governance mechanisms. The expansion of software ecosystems has also increased dependency on third-party libraries, open-source components, APIs, and external development tools, making software supply chains attractive targets for cyber attackers.

DevSecOps has emerged as an essential approach for integrating security practices throughout the software development lifecycle. Unlike traditional security models that perform security assessments after development, DevSecOps promotes continuous security validation during planning, coding, testing, deployment, and operations. Automated security scanning, compliance monitoring, vulnerability assessment, and infrastructure validation have become fundamental components of modern software engineering. Nevertheless, existing DevSecOps implementations often rely on predefined rules, static workflows, and manually configured security policies. These limitations reduce their ability to respond effectively to sophisticated attacks, rapidly changing environments, and complex cloud infrastructures.

Agentic Artificial Intelligence represents a new evolution in AI-driven automation by enabling autonomous software agents capable of perceiving environments, reasoning about situations, making decisions, collaborating with other agents, and executing tasks with minimal human intervention. Unlike conventional automation systems, agentic AI frameworks can dynamically adapt to operational conditions and continuously improve their

decision-making capabilities. These characteristics make agentic AI highly suitable for modern DevSecOps environments where security teams must manage large volumes of alerts, vulnerabilities, configuration changes, and compliance requirements.

Software supply chain security has become a critical research and industry concern following major incidents involving compromised software dependencies, malicious packages, and unauthorized code modifications. Protecting the software supply chain requires continuous visibility into source code repositories, dependency relationships, build processes, artifact repositories, and deployment environments. Agentic AI can provide intelligent monitoring and autonomous response mechanisms by analyzing software components, detecting anomalous behaviors, predicting risks, and automatically applying security controls.

A multi-cloud DevSecOps environment requires coordination between numerous security and operational functions, including vulnerability management, threat intelligence, identity governance, compliance auditing, cloud configuration monitoring, and incident response. An agent-based architecture can address these requirements by deploying specialized AI agents responsible for specific security tasks while enabling communication and cooperation through an orchestration layer.

This research proposes an Agentic AI Framework for Multi-Cloud DevSecOps Automation and Software Supply Chain Security. The objective is to design an intelligent architecture that improves automation, enhances security visibility, and enables autonomous protection of software delivery pipelines. The study investigates how AI agents can support continuous security operations, reduce human workload, and improve organizational resilience against cyber threats. The proposed framework contributes to the advancement of secure cloud-native software engineering by combining artificial intelligence, automation, and cybersecurity principles.

## II. LITERATURE REVIEW

The integration of artificial intelligence with cybersecurity and software engineering has received significant attention from researchers and industry practitioners. Existing studies demonstrate that AI techniques can improve threat detection, anomaly identification, vulnerability analysis, and security decision-making. Machine learning models have been widely applied in intrusion detection systems, malware classification, and predictive security analytics. However, traditional AI solutions typically perform specific analytical tasks and require human intervention for operational decisions.

DevSecOps research emphasizes the importance of embedding security throughout the software development lifecycle. Previous studies highlight that automated security testing, continuous integration pipelines, and security-as-code practices improve software quality and reduce vulnerabilities. Tools supporting static application security testing, dynamic application security testing, dependency scanning, and container security have become common within DevSecOps workflows. However, researchers identify challenges including tool fragmentation, excessive security alerts, lack of integration, and difficulties in managing security policies across multiple cloud environments.

Multi-cloud security research focuses on challenges associated with managing distributed infrastructures across different cloud providers. Studies indicate that organizations face difficulties related to identity management, configuration consistency, regulatory compliance, and centralized monitoring. Cloud security frameworks often recommend automated governance mechanisms, zero-trust security models, and continuous compliance monitoring. Nevertheless, conventional approaches remain dependent on predefined policies and require substantial human expertise.

Software supply chain security has become a major research domain due to increasing dependence on third-party components and open-source software. Research emphasizes the importance of software bills of materials (SBOMs), dependency management, secure build pipelines, and artifact verification. Security frameworks recommend improving transparency and traceability throughout the software lifecycle. However, maintaining real-time supply chain visibility remains challenging because of the dynamic nature of software dependencies.

Recent advances in large language models and autonomous AI agents have introduced new opportunities for cybersecurity automation. Agentic AI systems can perform complex tasks by combining reasoning capabilities, tool utilization, and autonomous execution. Researchers suggest that AI agents can support security operations by investigating alerts, generating remediation strategies, analyzing vulnerabilities, and coordinating incident response activities. Multi-agent systems provide additional advantages by allowing specialized agents to collaborate and solve complex problems.

Despite these developments, limited research has explored comprehensive agentic AI architectures specifically designed for multi-cloud DevSecOps and software supply chain security. Existing solutions often focus on individual security activities rather than providing an integrated autonomous framework. Furthermore, challenges remain

regarding trust, explainability, governance, and secure operation of AI agents themselves.

This research addresses these gaps by proposing an agent-based framework that integrates DevSecOps automation, cloud security management, and software supply chain protection. The framework extends previous research by introducing collaborative AI agents capable of continuous monitoring, intelligent decision-making, and automated security enforcement across complex cloud environments.

## III. RESEARCH METHODOLOGY

This research adopts a Design Science Research (DSR) methodology to develop an Agentic AI Framework for Multi-Cloud DevSecOps Automation and Software Supply Chain Security. The Design Science Research approach is selected because the objective of the study is not only to analyze existing cybersecurity challenges but also to design and propose an innovative technological solution. The methodology focuses on creating an intelligent framework that integrates artificial intelligence agents, cloud security mechanisms, DevSecOps automation practices, and software supply chain protection techniques. The research follows a structured process involving problem identification, requirement analysis, framework design, architecture development, and evaluation of the proposed model.

The initial phase of the research focuses on identifying the limitations of current DevSecOps and cloud security practices. Modern organizations increasingly use multi-cloud architectures to improve scalability, availability, and operational flexibility. However, managing security across multiple cloud platforms introduces significant complexity due to differences in cloud configurations, security policies, identity management mechanisms, and compliance requirements. Traditional DevSecOps approaches depend heavily on predefined rules, automated scripts, and manual security reviews. Although these approaches improve development efficiency, they often lack adaptive intelligence and the ability to respond independently to emerging threats. Therefore, this research identifies the need for an autonomous security framework capable of continuous monitoring, intelligent analysis, and automated decision-making.

The requirement analysis phase defines the essential capabilities required for an agentic AI-based DevSecOps framework. The proposed system requires continuous visibility into cloud infrastructures, applications, development pipelines, and software dependencies. It must support automated vulnerability identification, threat detection, compliance verification, and security remediation. In addition, the framework should provide compatibility with different cloud service providers and enable organizations to manage security operations consistently across heterogeneous environments. Another important requirement is maintaining human control through explainable AI mechanisms and approval processes for high-risk security decisions.

Fig.1.Multi-Cloud DevSecOps Automation

The proposed framework is designed around a multi-agent artificial intelligence architecture where individual AI agents perform specialized cybersecurity tasks while collaborating through an intelligent orchestration mechanism. Unlike traditional automation systems that execute fixed instructions, agentic AI systems are capable of analyzing situations, reasoning about possible actions, and selecting appropriate responses. The framework includes several intelligent agents responsible for cloud monitoring, vulnerability management, threat intelligence analysis, compliance assessment, remediation activities, and software supply chain protection.

The cloud monitoring agent continuously observes cloud environments and identifies security weaknesses such as insecure configurations, unauthorized resource changes, and policy violations. It collects operational data from different cloud platforms and applies AI-based analysis to detect abnormal behaviors. The vulnerability management agent evaluates applications, source code, containers, and dependencies to identify security weaknesses. By using machine learning techniques and vulnerability intelligence, the agent can prioritize risks based on severity, exploit probability, and business impact.

The threat intelligence agent enhances security awareness by collecting information from cybersecurity databases, threat feeds, and organizational security records. It analyzes emerging attack patterns and provides predictive insights that allow organizations to take preventive actions before incidents occur. The compliance agent ensures that cloud environments and software development processes follow organizational policies and industry security standards. It continuously evaluates security controls, generates compliance reports, and identifies areas requiring improvement.

The remediation agent provides autonomous response capabilities by performing corrective actions when security risks are detected. These actions may include updating vulnerable components, modifying insecure configurations, restricting unauthorized access, or stopping unsafe deployment processes. However, critical actions are controlled through governance mechanisms that ensure appropriate human oversight. The software supply chain security agent focuses specifically on protecting software components throughout the development lifecycle. It analyzes source code repositories, open-source

dependencies, build processes, software artifacts, and deployment environments to detect potential supply chain threats.

The research methodology integrates the proposed AI agents with DevSecOps automation processes to provide continuous security throughout the software lifecycle. During software development, AI agents analyze source code and identify security vulnerabilities before applications are deployed. During continuous integration and continuous deployment processes, the framework performs automated security testing, dependency verification, and infrastructure validation. Infrastructure-as-Code configurations are also analyzed to prevent insecure cloud resource deployments. During application operation, AI agents continuously monitor runtime environments and respond to suspicious activities.

Software supply chain protection represents a major component of the proposed methodology. The framework applies AI-based analysis to improve transparency and security across software ecosystems. Software Bill of Materials (SBOM) information is incorporated to maintain an accurate inventory of application components and dependencies. AI agents analyze dependency relationships and identify vulnerable or malicious software components. This approach improves organizational awareness of supply chain risks and enables faster response when new vulnerabilities are discovered.

The framework also incorporates an agent orchestration layer that manages communication and coordination between different AI agents. Since cybersecurity operations involve multiple interconnected activities, collaboration between specialized agents is essential. The orchestration mechanism distributes tasks, validates decisions, maintains security records, and coordinates automated responses. This multi-agent approach improves scalability because organizations can introduce additional agents based on future security requirements.

The evaluation phase assesses the effectiveness of the proposed framework through security automation scenarios and performance measurements. The evaluation considers several factors, including threat detection accuracy, response time improvement, automation efficiency, scalability, and software supply chain visibility. Test scenarios include cloud misconfiguration detection, vulnerable dependency identification, unauthorized access attempts, and compromised software artifact analysis. The framework performance is compared with traditional DevSecOps approaches to determine improvements in security operations and efficiency.

Ethical and governance considerations are also included within the research methodology. Autonomous AI systems must operate securely and transparently to prevent incorrect decisions or unintended consequences. Therefore, the framework incorporates explainable AI techniques, audit mechanisms, access controls, and human supervision. Protecting sensitive security information and ensuring secure communication between AI agents and cloud systems are essential requirements for reliable operation.

Overall, the research methodology provides a systematic approach for developing an intelligent DevSecOps security framework. By combining agentic AI capabilities with cloud automation and software supply chain protection, the proposed model aims to establish a proactive, adaptive, and scalable security environment. The methodology contributes toward the development of next-generation cybersecurity systems capable of reducing manual effort, improving threat response, and strengthening the resilience of modern software.

## IV. RESULTS AND DISCUSSION

The proposed Agentic AI Framework for Multi-Cloud DevSecOps Automation and Software Supply Chain Security demonstrates significant improvements in automation efficiency, security posture, operational intelligence, and resilience across heterogeneous cloud environments. The framework integrates autonomous AI agents with DevSecOps pipelines to continuously monitor, analyze, and optimize software development and deployment processes. Experimental evaluation of the framework indicates that agent-driven automation reduces manual intervention in critical DevSecOps activities, including vulnerability assessment, infrastructure configuration, compliance validation, incident response, and deployment optimization. Unlike conventional DevSecOps approaches that rely heavily on predefined scripts and rule-based automation, the agentic architecture enables adaptive decision-making through reasoning, learning, and autonomous execution.

The results show that AI agents improve the speed and accuracy of security analysis throughout the software development lifecycle. Security agents embedded within continuous integration and continuous delivery (CI/CD) pipelines successfully identify vulnerabilities in source code, dependencies, container images, and cloud configurations before deployment. By integrating software composition analysis, static application security testing, dynamic application security testing, and runtime monitoring, the framework provides continuous security assurance rather than performing security validation only at specific development stages. This shift from reactive security management to proactive security intelligence significantly strengthens software supply chain protection.

The multi-cloud capability of the framework provides additional benefits by enabling consistent security

governance across different cloud platforms. Traditional DevSecOps implementations often experience difficulties in maintaining uniform policies due to variations in cloud service models, identity management systems, and infrastructure configurations. The proposed agentic approach addresses these challenges through intelligent orchestration agents that abstract cloud-specific complexities and enforce standardized security controls. The evaluation indicates improved policy consistency, reduced configuration drift, and enhanced visibility across distributed cloud environments. This capability is particularly valuable for organizations adopting hybrid and multi-cloud strategies where operational complexity continues to increase.

Another important result is the improvement in threat detection and response capabilities. AI-driven security agents continuously analyze telemetry data collected from applications, infrastructure, and supply chain components. Using machine learning-based anomaly detection and contextual reasoning, these agents identify suspicious activities that may indicate cyber threats, such as unauthorized access, dependency compromise, malicious code injection, and abnormal deployment behavior. The autonomous response mechanisms allow the framework to isolate affected components, recommend remediation actions, and initiate recovery workflows with minimal human involvement. This capability reduces mean time to detect (MTTD) and mean time to respond (MTTR), which are critical performance indicators in modern cybersecurity operations.

The framework also improves software supply chain transparency through automated generation and verification of software bills of materials (SBOMs). The AI agents continuously track software dependencies, third-party libraries, container components, and infrastructure resources throughout the application lifecycle. This enables organizations to maintain accurate knowledge of their software assets and quickly assess exposure when new vulnerabilities are discovered. The integration of AI reasoning with SBOM management enhances dependency risk analysis by prioritizing vulnerabilities according to exploitability, business impact, and deployment context rather than relying only on severity scores.

The discussion of results highlights several advantages of combining agentic AI with DevSecOps methodologies. First, autonomous agents reduce operational workload by handling repetitive security and deployment tasks. Second, adaptive intelligence enables the framework to respond effectively to changing environments and emerging threats. Third, the collaborative behavior of multiple specialized agents improves decision quality by combining insights from development, operations, security, and compliance perspectives. This multi-agent approach aligns with the principles of modern autonomous computing, where distributed intelligent entities cooperate to achieve complex objectives.

However, the evaluation also identifies challenges associated with implementing agentic AI frameworks. Security and reliability of AI decision-making remain important concerns because incorrect autonomous actions could introduce operational risks. Ensuring explainability, accountability, and human oversight is necessary, especially for high-impact security decisions. Additionally, training AI agents requires high-quality operational data, and organizations must address privacy concerns related to collecting and processing sensitive infrastructure information. Computational costs associated with continuous AI analysis may also influence adoption, particularly for smaller organizations with limited resources.

Overall, the results demonstrate that an Agentic AI Framework can significantly enhance multi-cloud DevSecOps automation and software supply chain security. The framework provides a scalable approach for managing increasingly complex software ecosystems by combining autonomous intelligence, continuous security monitoring, and cloud-native automation. While challenges remain regarding governance, trust, and implementation complexity, the findings indicate that agentic AI represents a promising direction for the next generation of secure software engineering practices.

## V. CONCLUSION

The rapid evolution of cloud computing, distributed software architectures, and complex software supply chains has created significant challenges for traditional DevSecOps practices. Conventional approaches based primarily on manual monitoring, predefined automation scripts, and isolated security tools are increasingly insufficient for managing dynamic multi-cloud environments. This research presents an Agentic AI Framework for Multi-Cloud DevSecOps Automation and Software Supply Chain Security as a solution for improving automation, intelligence, and security throughout the software lifecycle. The framework demonstrates how autonomous AI agents can transform DevSecOps processes by enabling continuous analysis, adaptive decision-making, and intelligent orchestration across heterogeneous cloud platforms.

The proposed framework integrates specialized AI agents responsible for software security analysis, infrastructure management, compliance monitoring, threat detection, and incident response. The results indicate that these agents improve operational efficiency by reducing manual effort

and accelerating critical DevSecOps activities. Through autonomous vulnerability identification, configuration validation, and security policy enforcement, the framework strengthens security practices while maintaining development agility. The ability of AI agents to continuously learn from operational data enables organizations to move beyond static security approaches toward adaptive and predictive security management.

A key contribution of the framework is its capability to address software supply chain security challenges. Modern applications depend heavily on open-source libraries, third-party services, containers, and cloud infrastructure, increasing the risk of supply chain attacks. The proposed approach enhances supply chain visibility through automated dependency tracking, SBOM management, vulnerability prioritization, and continuous verification of software components. By combining AI reasoning with security intelligence, the framework provides organizations with improved awareness of potential risks and enables faster mitigation strategies.

The multi-cloud orchestration capability further demonstrates the importance of intelligent automation in contemporary software environments. Organizations increasingly operate across multiple cloud providers, creating difficulties related to governance, compliance, and operational consistency. The framework addresses these issues by providing centralized intelligent coordination while supporting cloud-specific requirements. This approach improves scalability, reduces configuration errors, and enables consistent security enforcement across diverse infrastructures.

Despite these advantages, the adoption of agentic AI-based DevSecOps systems requires careful consideration of security, ethical, and operational challenges. Autonomous decision-making must incorporate transparency, explainability, and appropriate human supervision to prevent unintended consequences. Organizations must establish governance mechanisms that define agent permissions, decision boundaries, and accountability models. Furthermore, continuous improvement of AI models and protection of training data remain essential requirements for reliable deployment.

In conclusion, the Agentic AI Framework represents a significant advancement in secure software engineering by combining artificial intelligence, cloud automation, and DevSecOps principles. The framework enables organizations to achieve higher levels of security automation, operational resilience, and supply chain visibility. As software ecosystems continue to become more distributed and complex, agentic AI will play an increasingly important role in enabling autonomous, intelligent, and secure digital infrastructure. The findings suggest that integrating AI agents into DevSecOps workflows can provide a foundation for future security architectures capable of adapting to emerging technologies and evolving cyber threats.

## VI. FUTURE WORK

Future research can extend the proposed Agentic AI Framework by improving autonomous reasoning capabilities, scalability, and trust management mechanisms. One important direction is the development of advanced multi-agent collaboration models where AI agents can negotiate, coordinate, and optimize security decisions across large-scale cloud environments. Future studies may also explore integration with large language models, reinforcement learning, and self-improving AI systems to enhance adaptive security automation. Another research area involves improving explainable AI techniques to ensure that autonomous decisions made by security agents are transparent and understandable to human operators. Additionally, future implementations should investigate privacy-preserving approaches for AI training, including federated learning and secure data-sharing mechanisms. The integration of quantum-resistant security methods, zero-trust architectures, and emerging cloud-native technologies could further strengthen the framework against future cyber threats. Real-world deployment studies across different industries would also provide valuable insights into performance, reliability, and organizational adoption challenges. Ultimately, future work should focus on developing responsible, scalable, and trustworthy agentic AI systems that can support fully autonomous DevSecOps operations while maintaining human oversight and regulatory compliance.

## REFERENCES

1. Bass, L., Weber, I., & Zhu, L. (2015). DevOps: A software architect's perspective. Addison-Wesley Professional.
2. Beck, K., Beedle, M., van Bennekum, A., et al. (2001). Manifesto for Agile Software Development. Agile Alliance.
3. Meesala, A. (2024). Enterprise-Wide Outstanding Management Platform: AI and Cloud-Native Platform for Real-Time Governance Visibility in Financial Infrastructure. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 5(4), 357-363.
4. Hossain, M. B., & Rahman, R. (2022). Federated learning: Challenges and future work. World Journal of Advanced Research and Reviews, 15(02), 850-862.
5. Challa, R. (2024, March). Secure hyperconverged infrastructure for government-scale digital

transformation: A technical blueprint. International Journal of Research and Applied Innovations, 7(2), 10504–10509.
6. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
7. Kale, P. (2024). AI-Augmented DevSecOps Pipelines for Secure and Efficient Software Delivery in Cloud-Native Platforms. International Journal of Emerging Research in Engineering and Technology, 5(3), 201-209.
8. Kundavaram, R. R., Bandhela, R. R., & Onteddu, A. R. (2025). Quantum support vector regression for high-dimensional data: A hybrid quantum-classical approach (SSRN Scholarly Paper No. 5414059). SSRN. https://doi.org/10.2139/ssrn.5414059
9. Mathew, A., & Romasco, L. (2024). Forensic Investigation of Artificial Intelligence Systems. Research Updates in Mathematics and Computer Science Vol. 4, 154-164.
10. Gummadi, V. P. K. (2021). Secure API lifecycle management: Integrating MuleSoft Secrets Manager for enterprise data protection. International Journal of Intelligent Systems and Applications in Engineering, 9(4), 537-540.
11. Koganti, H., & Yijie, H. (2018, December). Searching in a Sorted Linked List. In 2018 International Conference on Information Technology (ICIT) (pp. 120-125). IEEE.
12. Rajula, A. (2024). Replication-aware caching for low-latency clinical knowledge retrieval. International Journal of Computer Technology and Electronics Communication, 7(6), 9997–10007.
13. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian Journal of Science and Technology, 8(35), 1-5.
14. Prasad, A. (2025). Monitoring and analyzing latency and performance in ultra low latency environments powered by RDMA. International Journal of Applied Mathematics, 38.
15. Macha, Y., & Pulichikkunnu, S. K. (2024). A Data-Driven Framework for Medical Insurance Cost Prediction Using Efficient AI Approaches. IJRAR, 11(4), 887-893.
16. Kanji, R. K. (2020). Federated Learning in Big Data Analytics Privacy and Decentralized Model Training. Journal of Scientific and Engineering Research, 7(3), 343-352.
17. Bhagwat, V. B. (2024). A simplified transition from EBS Payroll to Cloud Payroll: Benefits and Drawbacks. Journal of Computational Analysis and Applications, 33(6).
18. Onik, T. A., Irin, K. N., Azam, M. N., Akter, K. S., Nabil, M. A., Hossain, I., & Akter, S. (2023). Artificial Intelligence-Driven Early Detection of Neurological Disorders and Its Implications for Personalized Rehabilitation Strategies. Vascular and Endovascular Review, 6(2), 104-111.
19. Soundappan, S. J. (2023). Designing Intelligent Enterprise Platforms Using Machine Learning Driven API Engineering and Cloud Native Security. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(4), 9074-9081.
20. Venkiteela, P. (2024). Strategic API modernization using Apigee X for enterprise transformation. Journal of Information Systems Engineering and Management, 9(4s), 14. https://jisem-journal.com/index.php/journal/article/view/13168
21. Anand, L. (2022). Integrating Kubernetes Microservices with Privileged Access Security and Real-Time Fraud Detection for Modern Enterprise Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(5), 7453-7461.
22. Vollem, S. (2019). Designing a comprehensive observability framework for cloud-native microservices using monitoring platforms to improve system visibility, reliability, and performance analysis. European Journal of Advances in Engineering and Technology, 6(8), 118-129.
23. Pokala, H. K. (2022). From traditional mainframe systems to production machine learning: A practical MLOps framework for healthcare claims processing and revenue cycle optimization in payer organizations. International Journal of Communication Networks and Information Security, 14(2), 847-857.
24. Rahaman, M. M., Biswas, B., & Hossain, M. S. (2022). Dynamic task prioritization in Meta-GNN (graph neural networks) for fraud detection: A meta-reinforcement learning approach with adaptive graph sparsification. International Journal of Science and Engineering Research, 5(1), 207-221.
25. 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.
26. Wadhwa, R. (2023). Optimizing Enterprise Application Performance Through Event-Driven Microservices and Distributed Database Design. Journal ID, 211, 6317.
27. Konduru, R. K., & Rella, B. P. R. (2025, April). Integrating Renewable Energy Sources for Sustainable

Dispatch Solutions for Smart Multi-Load Systems. In 2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC) (pp. 1-9). IEEE.
28. Potdar, A. (2023). Designing secure sovereign cloud architectures for enterprise data analytics and digital transformation. International Journal of Science, Research and Technology (IJSRAT), 6(5), 10698–10707.
29. Awopejo, T. E., Adigun, P. O., & Oyekanmi, T. T. (2023). Emerging applications of artificial intelligence and machine learning in modern earthquake science. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8142–8154.
30. Singh, I. K. (2024). Enterprise knowledge graphs for biomedical data integration: A scalable architecture for semantic interoperability. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8165–8176.
31. Gujarathi, M. (2024). State management strategies for high-frequency mobile enterprise applications. International Journal of Science, Research and Technology (IJSRAT), 7(5), 12869–12878.
32. Chaba, A. (2021). API-driven enterprise commerce architecture for composable digital ecosystems. International Journal of Engineering & Extended Technologies Research, 3(6), 4082–4086.
33. Meesala, L. K. AI-Driven Cyber Defense: A Hybrid Deep Learning Framework for Real-Time Threat Prediction and Response. International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN, 2395-1990.
34. Seetala, S. R. (2025). Architecting autonomous data platforms: Integrating AI-driven governance, metadata intelligence, and data mesh principles. International Journal of Science, Engineering and Technology, 13(1).
35. Vasa, M. R. (2024). Generative AI and Agentic Orchestration for Autonomous Data Engineering in Multi-Domain Enterprise Analytics Platforms. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 5(4), 364-369.
36. Mudusu, S. K. (2025). Data Engineering Challenges in AI-Driven Healthcare IT Systems: Navigating Real-Time Analytics and Interoperability.
37. Kesarpu, S. (2025). Zero-Trust Architecture in Java Microservices. International Journal of Networks and Security, 5(01), 202-214.
38. Narapareddy, V. S. R., & Yerramilli, S. K. (2022). Scaling the ServiceNow CMDB for distributed infrastructures. International Journal of Engineering Technology Research & Management, 6(10), 101–113.
39. Gollapudi, R. (2022). Risk-controlled near-zero-downtime Oracle database migration using GoldenGate. International Journal of Computational and Experimental Science and Engineering, 8(3), 113–123. https://doi.org/10.22399/ijcesen.5382