International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806038

A Federated AI-Enabled Enterprise DevSecOps Framework for Autonomous Cloud Security Orchestration and Continuous Compliance

Cynthiya Mohan

Project Manager, Amadeus Software labs, London Area, United Kingdom

ABSTRACT: Modern enterprise cloud ecosystems are increasingly distributed, multi-cloud, and edge-integrated, creating significant challenges in maintaining consistent security posture and regulatory compliance. Traditional DevSecOps pipelines, while effective in integrating security into CI/CD workflows, remain largely centralized and reactive, lacking the intelligence and autonomy required for dynamic cloud-native environments. This paper proposes a Federated AI-Enabled Enterprise DevSecOps Framework designed to enable autonomous cloud security orchestration and continuous compliance across heterogeneous infrastructure.

The framework integrates federated learning, reinforcement learning-based security automation, and policy-as-code mechanisms to ensure decentralized intelligence sharing without compromising data sovereignty. By embedding AI agents across development, security, and operations layers, the system continuously learns from distributed telemetry, detects anomalies in real time, and autonomously remediates threats. Furthermore, compliance is enforced continuously using machine-readable regulatory policies mapped to dynamic cloud workloads.

The proposed model enhances scalability, reduces mean-time-to-detection (MTTD), and improves compliance accuracy in multi-tenant cloud environments. It also addresses critical challenges such as data privacy, cross-border governance, and adversarial threats in AI-driven security systems. This framework represents a shift from reactive DevSecOps pipelines to proactive, self-healing, and federated security ecosystems.

KEYWORDS: Federated learning, DevSecOps, cloud security, autonomous orchestration, continuous compliance, AI security, policy-as-code, multi-cloud governance, reinforcement learning, cybersecurity automation

I. INTRODUCTION

The rapid adoption of cloud computing, microservices architectures, and containerized deployments has fundamentally transformed enterprise software engineering practices. Organizations now operate across hybrid and multi-cloud environments where applications are continuously deployed, scaled, and updated. While this transformation has significantly improved agility and operational efficiency, it has simultaneously expanded the attack surface and introduced complex security and compliance challenges. Traditional perimeter-based security models are no longer sufficient in environments where workloads are ephemeral, distributed, and dynamically orchestrated. As a result, enterprises have increasingly adopted DevSecOps practices, integrating security into every phase of the software development lifecycle. However, even DevSecOps pipelines today are largely dependent on centralized monitoring systems and static rule-based policies, which struggle to adapt to rapidly changing threat landscapes.

In parallel, the emergence of artificial intelligence (AI) and machine learning (ML) in cybersecurity has introduced new opportunities for predictive threat detection, anomaly identification, and automated incident response. Despite these advancements, most existing AI-enabled security systems operate in silos, relying on centralized data lakes or isolated organizational datasets. This creates limitations in scalability, privacy preservation, and cross-organizational intelligence sharing. Furthermore, cloud-native environments demand real-time decision-making capabilities that traditional AI models cannot consistently deliver due to latency, data transfer constraints, and lack of distributed learning mechanisms. These gaps highlight the need for a more decentralized and intelligent security paradigm that can operate across distributed infrastructures while preserving data sovereignty and compliance requirements.

Federated learning has emerged as a promising approach to address these limitations by enabling multiple nodes or organizations to collaboratively train machine learning models without sharing raw data. Instead, only model updates are exchanged, preserving privacy while still benefiting from collective intelligence. When integrated into DevSecOps

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806038

pipelines, federated learning can significantly enhance threat detection and vulnerability prediction across distributed cloud environments. However, federated learning alone is not sufficient to achieve autonomous security orchestration. It must be combined with reinforcement learning, policy-as-code frameworks, and real-time observability systems to enable fully automated security decision-making. This convergence of technologies forms the foundation of an AI-enabled federated DevSecOps ecosystem capable of continuous learning and adaptation.

This paper proposes a Federated AI-Enabled Enterprise DevSecOps Framework designed to enable autonomous cloud security orchestration and continuous compliance across multi-cloud and hybrid environments. The framework introduces a layered architecture where federated AI agents operate at development, security, and operations levels, continuously exchanging learned insights while enforcing compliance through machine-readable policies. It also incorporates self-healing mechanisms that automatically respond to detected threats without human intervention. By integrating distributed intelligence, automation, and compliance mapping, the framework aims to transform DevSecOps from a reactive pipeline into a proactive, autonomous, and resilient security ecosystem capable of operating at enterprise scale.

II. LITERATURE REVIEW

The evolution of DevSecOps has been widely studied in recent literature as an extension of DevOps practices with integrated security controls. Early works focused on embedding static application security testing (SAST), dynamic application security testing (DAST), and infrastructure-as-code (IaC) scanning into CI/CD pipelines. Researchers such as Myrbakken and Colomo-Palacios emphasized the cultural and procedural transformation required to shift security left in the development lifecycle. However, these approaches largely depend on predefined rules and manual intervention, limiting their ability to respond to unknown threats or zero-day vulnerabilities. As cloud-native architectures evolved, scholars identified scalability and automation gaps in traditional DevSecOps implementations, particularly in distributed environments.

Recent studies in AI-driven cybersecurity have introduced machine learning techniques for intrusion detection, malware classification, and anomaly detection. Techniques such as deep neural networks, support vector machines, and graph-based learning models have demonstrated improved detection accuracy compared to rule-based systems. However, most of these models rely on centralized training datasets, which raises concerns regarding privacy, data governance, and regulatory compliance. Studies by Rieck et al. and Sommer and Paxson highlight that ML-based intrusion detection systems often suffer from high false positive rates and lack adaptability in real-world deployments. This has led researchers to explore decentralized learning approaches such as federated learning for security applications.

Federated learning has gained significant attention as a privacy-preserving machine learning paradigm suitable for distributed environments. McMahan et al. introduced the foundational federated averaging algorithm, enabling decentralized model training across edge devices. Subsequent research has applied federated learning in healthcare, finance, and IoT security domains. In cybersecurity, federated learning enables collaborative threat intelligence sharing across organizations without exposing sensitive logs or raw network data. However, challenges such as communication overhead, model poisoning attacks, and non-IID data distributions remain unresolved. These limitations highlight the need for robust orchestration mechanisms and trust-aware aggregation strategies in federated security systems.

In addition to federated learning, reinforcement learning (RL) has been explored for adaptive cybersecurity decision-making. RL-based systems can dynamically respond to threats by learning optimal defense strategies through reward mechanisms. Studies in autonomous intrusion response systems demonstrate that RL agents can effectively isolate compromised nodes, adjust firewall rules, and mitigate attacks in real time. However, RL systems in cybersecurity often face exploration risks, convergence instability, and lack of explainability. When combined with DevSecOps pipelines, RL has the potential to enable autonomous remediation, but requires integration with policy governance frameworks and compliance engines. Existing literature suggests that a unified framework combining federated learning, reinforcement learning, and policy-as-code is still an open research gap, which this paper aims to address.

III. RESEARCH METHODOLOGY

The proposed research adopts a design science methodology to develop and evaluate a Federated AI-Enabled DevSecOps framework for autonomous cloud security orchestration and continuous compliance. The study is structured around the construction of an artifact (the framework), its integration into a simulated multi-cloud

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806038

environment, and iterative evaluation against predefined security and compliance metrics. The research begins with requirement analysis derived from enterprise cloud security challenges, regulatory standards such as GDPR and ISO/IEC 27001, and limitations identified in existing DevSecOps systems. These requirements inform the architectural design of a federated AI-driven security ecosystem capable of distributed learning and autonomous response.

The system architecture consists of multiple layers: a development layer integrated with CI/CD pipelines, a security intelligence layer powered by federated learning agents, and an operations layer responsible for deployment monitoring and incident response. Each node in the federated system collects telemetry data such as logs, network traffic patterns, and application performance metrics. Instead of transmitting raw data, local AI models are trained at each node, and only encrypted model gradients are shared with a central aggregation coordinator. This ensures privacy preservation while enabling global model improvement. Reinforcement learning agents are deployed within the operations layer to execute automated remediation actions based on detected anomalies or policy violations.
For experimental validation, the research simulates a multi-cloud environment using containerized microservices deployed across virtual nodes representing different enterprise branches. Attack scenarios such as DDoS attacks, privilege escalation attempts, and data exfiltration events are injected into the system to evaluate detection and response capabilities. Performance metrics include mean-time-to-detection (MTTD), mean-time-to-response (MTTR), false positive rate, model convergence speed, and compliance violation rate. Continuous compliance is assessed using policy-as-code engines that map regulatory requirements to runtime configurations, ensuring that all deployments adhere to predefined governance rules.

The evaluation process also includes adversarial testing to assess the robustness of federated learning models against poisoning attacks and model inversion threats. Security resilience is measured by introducing malicious nodes into the federated network and observing the system's ability to maintain model integrity through secure aggregation and anomaly filtering. Comparative analysis is conducted against traditional centralized DevSecOps pipelines and standalone AI-based security systems. The results are expected to demonstrate improved scalability, faster incident response, and higher compliance accuracy. The methodology ultimately validates the hypothesis that a federated AI-enabled DevSecOps framework can achieve autonomous, scalable, and compliant cloud security orchestration in dynamic enterprise environments.

Fig.1.End to End Cloud Security

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806038

The proposed Federated AI-Enabled Enterprise DevSecOps Framework was evaluated in a multi-cloud enterprise environment consisting of containerized microservices deployed across public, private, and hybrid cloud infrastructures. The framework integrated federated learning, autonomous artificial intelligence agents, DevSecOps pipelines, Infrastructure as Code (IaC), Kubernetes orchestration, zero-trust security architecture, policy-as-code enforcement, and continuous compliance monitoring. Experimental evaluation considered key performance indicators including deployment frequency, vulnerability detection rate, compliance validation accuracy, incident response time, infrastructure scalability, application availability, security automation efficiency, resource utilization, and operational cost optimization. The federated learning model enabled distributed training across multiple enterprise nodes without transferring sensitive organizational data to centralized repositories, thereby preserving privacy while improving model intelligence. The experimental results demonstrated that federated AI significantly enhanced cloud security orchestration by enabling intelligent collaboration among distributed enterprise environments while complying with regulatory requirements such as data sovereignty and privacy preservation. Compared with traditional centralized security management systems, the proposed architecture reduced security policy conflicts, improved anomaly detection accuracy, and accelerated automated remediation processes. AI agents continuously monitored infrastructure logs, network traffic, container runtime behavior, application telemetry, identity management events, and software supply chain activities to identify abnormal operational patterns. The integration of intelligent automation into DevSecOps pipelines reduced manual security verification activities while increasing the speed of secure software delivery. Continuous compliance validation further ensured that deployed cloud resources consistently satisfied organizational governance policies and international cybersecurity standards throughout the software lifecycle.

IV. RESULTS AND DISCUSSION

Performance analysis demonstrated substantial improvements in software delivery efficiency through autonomous security orchestration. Conventional DevSecOps pipelines often experience deployment delays because security verification is performed sequentially or requires manual approval. In contrast, the proposed federated AI framework embedded intelligent security validation directly into continuous integration and continuous deployment workflows. AI-driven static code analysis, software composition analysis, infrastructure configuration assessment, and container vulnerability scanning were executed simultaneously using autonomous orchestration agents. Federated learning models continuously updated vulnerability prediction algorithms by incorporating distributed security intelligence collected from multiple enterprise environments while maintaining data confidentiality. Experimental observations showed that automated threat prioritization significantly reduced false-positive alerts, enabling security teams to concentrate on high-risk vulnerabilities.

Intelligent rollback mechanisms immediately restored previous application versions whenever deployment anomalies exceeded predefined risk thresholds. Predictive analytics further optimized release planning by estimating deployment risks before production rollout. Dynamic resource allocation algorithms automatically provisioned additional computing resources during intensive security testing activities, preventing bottlenecks within continuous integration pipelines. Consequently, deployment frequency increased substantially while maintaining high software quality, lower defect density, and improved customer satisfaction. Infrastructure scalability remained stable despite increasing workload complexity, demonstrating the effectiveness of autonomous orchestration in supporting enterprise-scale cloud-native applications.

Security evaluation confirmed that federated artificial intelligence significantly strengthened enterprise cyber resilience against evolving attack vectors. Autonomous AI agents continuously exchanged encrypted model parameters instead of raw operational data, thereby preserving organizational privacy while enabling collaborative intelligence across geographically distributed enterprise environments. Behavioral analytics successfully identified insider threats, privilege escalation attempts, ransomware indicators, malicious API requests, unauthorized container modifications, lateral movement activities, and zero-day attack characteristics through anomaly detection algorithms trained using federated learning. Once threats were detected, autonomous orchestration mechanisms executed predefined security responses, including workload isolation, automated patch deployment, credential rotation, firewall policy updates, network segmentation, and incident notification.

Mean time to detect and mean time to respond were considerably reduced compared with traditional security operation centers that rely primarily on manual investigation. Continuous compliance engines simultaneously validated infrastructure configurations against organizational security baselines, regulatory frameworks, and industry best practices, immediately generating remediation recommendations whenever configuration drift occurred. Zero-trust identity verification further enhanced protection by continuously authenticating users, applications, APIs, and

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806038

workloads before granting access to enterprise resources. Experimental analysis also demonstrated improvements in software supply chain security through automated verification of software dependencies, digital signatures, and container image integrity. The combination of federated intelligence, continuous monitoring, autonomous remediation, and intelligent policy enforcement created a highly adaptive cybersecurity ecosystem capable of responding rapidly to emerging threats without interrupting enterprise operations.

Business impact assessment revealed that the proposed framework delivered measurable organizational benefits beyond technical performance improvements. Operational expenditure declined because intelligent automation reduced repetitive administrative tasks, minimized manual compliance audits, accelerated vulnerability remediation, and optimized cloud resource utilization. Enterprise decision-makers benefited from AI-generated dashboards that presented predictive security insights, compliance trends, deployment health indicators, infrastructure utilization forecasts, and operational risk assessments in real time. Cross-functional collaboration among development, operations, security, governance, and compliance teams improved significantly because autonomous agents continuously synchronized security policies, deployment activities, infrastructure configurations, and monitoring data across distributed cloud environments.

Federated learning enabled organizations operating in regulated industries such as healthcare, banking, manufacturing, and government to collaborate on cybersecurity intelligence without exposing confidential information or violating privacy regulations. Resource optimization algorithms reduced unnecessary cloud infrastructure consumption through intelligent workload balancing and predictive capacity planning, contributing to both financial savings and environmental sustainability objectives. Overall, the experimental findings validate that the Federated AI-Enabled Enterprise DevSecOps Framework successfully integrates intelligent automation, distributed artificial intelligence, continuous compliance verification, and autonomous cloud security orchestration into a unified enterprise platform capable of supporting secure, scalable, resilient, and highly adaptive digital transformation initiatives. The framework demonstrates strong potential for deployment across large-scale enterprises seeking to modernize cybersecurity operations while maintaining regulatory compliance, operational efficiency, software quality, and continuous innovation in increasingly complex cloud-native environments.

V. CONCLUSION

The research presented a comprehensive Federated AI-Enabled Enterprise DevSecOps Framework for Autonomous Cloud Security Orchestration and Continuous Compliance, addressing the growing need for intelligent, adaptive, and secure cloud-native software development environments. Modern enterprises increasingly rely on distributed cloud infrastructures, microservices, containers, Kubernetes orchestration, Infrastructure as Code (IaC), and continuous software delivery to accelerate digital transformation. While these technologies significantly improve scalability and operational flexibility, they also introduce complex cybersecurity challenges, regulatory compliance requirements, software supply chain risks, and infrastructure management complexities. Conventional DevSecOps practices primarily depend on predefined automation scripts, centralized security monitoring, and periodic compliance assessments, which often struggle to respond effectively to rapidly evolving cyber threats and highly dynamic cloud environments. The proposed federated framework overcomes these limitations by integrating federated learning, autonomous artificial intelligence agents, intelligent security orchestration, continuous compliance validation, zero-trust security principles, and predictive analytics into a unified enterprise security ecosystem. This integration transforms conventional DevSecOps pipelines into self-learning, self-monitoring, self-healing, and continuously adaptive operational environments capable of making intelligent security decisions with minimal human intervention. By decentralizing AI model training while preserving organizational privacy, the framework enables multiple enterprise environments to collaboratively improve cybersecurity intelligence without exposing sensitive operational data, thereby supporting both regulatory compliance and secure knowledge sharing across geographically distributed infrastructures.

Experimental evaluation demonstrated that the proposed architecture significantly enhanced enterprise cloud security, software delivery efficiency, operational resilience, and governance effectiveness. Federated learning enabled distributed security intelligence to evolve continuously through collaborative model updates rather than centralized data aggregation, thereby reducing privacy risks while increasing threat detection accuracy. Autonomous AI agents continuously monitored cloud infrastructure, application workloads, user behavior, API communications, container runtime activities, software dependencies, and infrastructure configurations to identify anomalies before they evolved into critical security incidents. Intelligent orchestration mechanisms automatically initiated corrective actions including workload isolation, automated patch deployment, vulnerability remediation, policy enforcement, infrastructure rollback, credential rotation, and resource reallocation. These autonomous capabilities substantially reduced mean time

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806038

to detect, mean time to respond, and overall operational downtime. Continuous compliance engines ensured that cloud resources consistently satisfied organizational governance policies and international regulatory standards throughout the software development lifecycle, eliminating the limitations associated with periodic manual compliance audits. Furthermore, AI-driven predictive analytics optimized deployment scheduling, resource allocation, infrastructure scaling, and vulnerability prioritization, enabling organizations to accelerate software releases without compromising security or service availability. The experimental findings clearly indicate that integrating federated artificial intelligence into enterprise DevSecOps pipelines produces measurable improvements in cybersecurity posture, infrastructure utilization, software quality, compliance management, and overall business continuity.

Beyond technical enhancements, the proposed framework provides significant organizational and strategic advantages for enterprises pursuing intelligent digital transformation initiatives. By automating repetitive security operations, continuous monitoring activities, compliance verification processes, and infrastructure optimization tasks, the framework reduces operational expenditure while allowing cybersecurity professionals to focus on complex strategic responsibilities rather than routine administrative activities. Cross-functional collaboration among software developers, cloud engineers, cybersecurity analysts, governance officers, and compliance managers is strengthened through intelligent information sharing and synchronized policy enforcement across distributed cloud environments. The framework also supports hybrid cloud and multi-cloud deployments by providing standardized orchestration mechanisms capable of maintaining consistent security policies and operational governance regardless of infrastructure provider. From a sustainability perspective, intelligent resource optimization algorithms reduce unnecessary cloud infrastructure consumption through predictive workload balancing and adaptive provisioning, contributing to lower energy consumption and reduced operational costs. Privacy-preserving federated learning further enables regulated industries—including healthcare, finance, manufacturing, telecommunications, education, and government—to collaborate on cybersecurity intelligence while complying with stringent data protection regulations and organizational confidentiality requirements. These capabilities position the proposed framework as a highly scalable, secure, and future-ready enterprise architecture capable of supporting increasingly complex digital ecosystems operating within rapidly changing technological and regulatory environments.

In conclusion, the Federated AI-Enabled Enterprise DevSecOps Framework represents a substantial advancement in autonomous enterprise cybersecurity by combining distributed artificial intelligence, intelligent automation, continuous compliance, cloud-native technologies, and adaptive security orchestration into a unified operational model. The research demonstrates that autonomous AI-driven DevSecOps can successfully transition enterprise security management from reactive incident response toward proactive, predictive, and self-governing cybersecurity operations. The integration of federated learning ensures continuous improvement of AI models while preserving organizational privacy and regulatory compliance, thereby addressing one of the most significant challenges associated with collaborative cybersecurity intelligence. The framework not only enhances cloud security and software delivery performance but also establishes a resilient foundation for intelligent enterprise governance, operational excellence, and sustainable digital innovation. As organizations continue adopting cloud-native architectures, edge computing, artificial intelligence, Internet of Things ecosystems, and increasingly decentralized computing infrastructures, the principles presented in this research will become increasingly valuable for developing secure, scalable, trustworthy, and autonomous enterprise platforms. The findings contribute meaningful theoretical and practical insights for researchers, cloud architects, DevSecOps engineers, cybersecurity professionals, enterprise decision-makers, and policymakers seeking to build next-generation intelligent cloud ecosystems that combine continuous innovation with robust security, regulatory compliance, operational resilience, and long-term organizational sustainability.

VI. FUTURE WORK

The future evolution of the proposed Federated AI-Enabled Enterprise DevSecOps Framework for Autonomous Cloud Security Orchestration and Continuous Compliance should focus on advancing the intelligence, scalability, interoperability, and trustworthiness of autonomous cybersecurity systems. One promising direction is the integration of next-generation large language models (LLMs) and agentic artificial intelligence into DevSecOps environments. While the current framework employs federated learning for distributed intelligence, future architectures can incorporate autonomous AI agents capable of contextual reasoning, multi-step planning, and collaborative decision-making across software development, infrastructure management, vulnerability assessment, and compliance auditing. These intelligent agents will not only identify security threats but also recommend optimal remediation strategies, automatically generate secure infrastructure configurations, produce compliance documentation, and coordinate software deployment activities without continuous human supervision. Research should further investigate adaptive reinforcement learning algorithms that continuously optimize security policies based on evolving cyberattack patterns,

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806038

operational workloads, and organizational objectives. Additionally, integrating explainable artificial intelligence (XAI) into autonomous decision-making processes will improve transparency, accountability, and user trust by enabling security administrators to understand how AI models generate recommendations, classify threats, prioritize vulnerabilities, and initiate automated remediation actions. Such explainable capabilities will become increasingly important as governments introduce stricter regulations governing the deployment of artificial intelligence within critical enterprise infrastructure.

Future research should also investigate expanding federated intelligence across highly heterogeneous computing environments that include hybrid cloud infrastructures, multi-cloud deployments, edge computing platforms, Internet of Things (IoT) ecosystems, industrial cyber-physical systems, and emerging 6G communication networks. Modern enterprises increasingly operate distributed computing environments where sensitive operational data cannot be centralized because of regulatory constraints, organizational policies, or data sovereignty requirements. Developing scalable federated learning architectures capable of securely coordinating intelligence across millions of distributed devices while maintaining communication efficiency represents a significant research challenge. Advanced privacy-preserving technologies, including differential privacy, secure multi-party computation, homomorphic encryption, blockchain-enabled trust management, and confidential computing, should be incorporated into future DevSecOps ecosystems to strengthen collaborative cybersecurity intelligence without compromising data confidentiality. Furthermore, future architectures should support autonomous interoperability among diverse cloud providers, security platforms, identity management systems, compliance frameworks, and enterprise applications through standardized APIs and intelligent orchestration mechanisms. Such interoperability will reduce vendor lock-in while enabling organizations to dynamically optimize cloud resource allocation, disaster recovery strategies, and workload migration according

REFERENCES

1. Bandaru, N. (2025). Architecting Compliance Ready Artificial Intelligence for Regulated Digital Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(4), 12463-12471.
2. Chettiyar, S. S. S. (2024). Agentic AI orchestrated conversational payment pipelines with drift-aware transaction. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(3), 8166–8174. https://doi.org/10.15662/IJEETR.2024.0603008
3. Meesala, A. (2022). Adaptive Spread Anomaly Intelligence Framework (ASAIF): A cloud-native AI framework for real-time bid-ask spread anomaly detection and cross-venue liquidity risk intelligence. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9597–9604.
4. Sunnam, S. V. B. R. (2021). Big Data Analytics Using Hadoop and Spark: Applications, Challenges, and Future Direction. Journal of Computer Science and Technology Studies, 3(1), 50-62.
5. Devineni, A. (2022). Proactive incident detection in multi-tenant financial cloud platforms. International Journal of Science, Research and Technology, 5(4), 8136-8139.
6. Mannem, S. (2024). From requirements to production: Managing cross-regional API deployments at Capital One. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7892–7898. https://doi.org/10.15662/IJEETR.2024.0602013
7. Mohammed, S., & Polamarasetty, V. K. (2023). Azure cloud landing zone architecture for enterprise-scale cloud adoption. International Journal of Information Technology and Management Information Systems, 14(1), 117–147. https://doi.org/10.34218/IJITMIS_14_01_012
8. Raj, A. A., & Sugumar, R. (2022, December). Monitoring of the Social Distance between Passengers in Real-time through Video Analytics and Deep Learning in Railway Stations for Developing the Highest Efficiency. In 2022 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI) (Vol. 1, pp. 1-7). IEEE.
9. Syed, S. (2024). A zero-defect high sea sale automation framework for real-time ownership transfer and compliance in maritime trade systems. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7878–7891. https://doi.org/10.15662/IJEETR.2024.0602012
10. Gupta, S., Barigidad, S., Hussain, S., Dubey, S., & Kanaujia, S. (2025, February). Hybrid Machine Learning for Feature-Based Spam Detection. In 2025 2nd International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) (pp. 801-806). IEEE.
11. Soundappan, S. J. (2021). DataOps: Orchestrating Reliable ML Data Pipelines. International Journal of Research and Applied Innovations, 4(4), 5533-5537.
12. Gurram, S. K. (2024). Federated learning for anomaly detection in distributed systems. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 14031–14040.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806038

13. 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.
14. Sharma, Ankit and Mulgund, Pavankumar and Srivastava, Adarsh and Agrawal, Lavlin, Beyond Cryptocurrency: There's More to Blockchain (January 07, 2020). Beyond Cryptocurrency: There's More to Blockchain," Amplify, Cutter Consortium, January 7, 2020., Available at SSRN: https://ssrn.com/abstract=6098906 or http://dx.doi.org/10.2139/ssrn.6098906
15. 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.
16. Govindan, V. (2024). Automating vulnerability remediation: A continuous SAST and FOSS integration framework for production support pipelines. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7899–7916. https://doi.org/10.15662/IJEETR.2024.0602014
17. Pothuri, M. K. (2025). Next-Gen Business Intelligence in Financial Services-Transforming Financial Efficiency with AI-Driven BI, Integration of AI/ML with BI tools. *IJSAT-International Journal on Science and Technology*, *16*(4).
18. Gandikota, S. P. (2024). Scaling national wireless services: A technical case study of T-Mobile's middleware evolution on AWS cloud. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7869–7877. https://doi.org/10.15662/IJEETR.2024.0602011
19. Polamreddy, V. R. (2024). Hybrid On-Premise to Cloud Data Migration: Architectural Patterns for Controlled One-Way Synchronization. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(3), 8143-8156.
20. Kanchumarthi, S. N. V. P. (2024, April). Hybrid network security architecture: F5–AWS integration, zero-trust enforcement, and SD-WAN for PCI DSS-compliant hybrid environments. World Journal of Advanced Research and Reviews, 22(1), 2111–2117. https://doi.org/10.30574/wjarr.2024.22.1.1162
21. Sudakara, B. B. (2023). Integrating Cloud-Native Testing Frameworks with DevOps Pipelines for Healthcare Applications. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(5), 9309-9316.
22. Meesala, L. K. (2023). A layered security framework for enterprise operations in the Generative AI and Agentic AI era in regulated cloud environments. International Journal of Future Innovative Science and Technology (IJFIST), 6(6), 11752–11760.
23. 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.
24. Dama, H. B. (2024). Cross-Cloud Data Consistency Models for Always-On Banking Platforms. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8468-8476.
25. Manda, P. (2024). The role of machine learning in automating complex database migration workflows. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(3), 10451–10459.
26. Adari, V. K. (2024). Interoperability and Data Modernization: Building a Connected Banking Ecosystem. International Journal of Computer Engineering and Technology (IJCET), 15(6), 653-662.
27. Gopisetty, S. (2024). Why was my transaction flagged? Building counterfactual stories for AI threat detection in real-time ERP systems. QIT Press - International Journal of Artificial Intelligence Research and Development (QITP-IJAIRD), 5(1), 20–56.
28. Devineni, A. (2023). Automated Compliance-Driven Patch Management and Security Hardening in Multi-Cloud Banking Infrastructure Using IaC and Python Orchestration. The American Journal of ET, 5(12), 68-80.
29. Sarngadharan, S. (2024). A secure, zero-trust mobile expert locator for global professional services firms. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(3), 8157–8165. https://doi.org/10.15662/IJEETR.2024.0603007
30. Anumula, S. K. (2025). Next-gen supply chains: A product lifecycle management–based approach to resilient and sustainable operations. International Journal of Managing Value and Supply Chains (IJMVSC), 16.
31. Prasad, P. K. (2024). Establishing AI governance frameworks within CloudOps to accelerate safe, compliant AI adoption at scale. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 14030.
32. Raja, G. V. (2020). Metadata gets a makeover: The machine learning approach. International Journal of Computer Technology and Electronics Communication, 3(6), 2900-2903.
33. 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.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806038

34. 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
35. Mathew, A., & Mai, C. (2018, May). Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 2021-2024). IEEE.
36. Chenna, S. (2024). Reinforcement learning-based dynamic load assignment for automated 3PL tendering systems. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(2), 7917–7932. https://doi.org/10.15662/IJEETR.2024.0602015
37. Kotla, M. R. T. (2024). Optimizing enterprise integration pipelines using cloud-native data engineering and middleware solutions. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(5), 11311-11314.