International Journal of Emerging Trends in Engineering and Management Research (IJETEMR)

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 9, Issue 5, September-October 2024|

DOI:10.15662/ijetemr.2024.0905002

Generative AI Enabled Enterprise Cloud Platforms for Intelligent Business Process Automation and Secure Data Integration

Dr Vimal Raja Gopinathan

Senior Principal Consultant, Oracle Financial Service Software Ltd, Washington, USA

ABSTRACT: Generative Artificial Intelligence (GenAI) is rapidly transforming enterprise cloud platforms by enabling intelligent automation, adaptive decision-making, and enhanced data integration across distributed systems. This paper explores a conceptual framework for integrating Generative AI into enterprise cloud environments to support intelligent business process automation and secure data management. Modern enterprises face challenges such as data silos, inconsistent workflows, security vulnerabilities, and limited adaptability in traditional automation systems. The proposed GenAI-enabled cloud platform addresses these challenges by combining large language models, cloud-native microservices, and secure data pipelines to enable autonomous process orchestration and real-time decision support. The architecture incorporates AI-driven workflow generation, intelligent API integration, and policy-based security enforcement to ensure scalability, resilience, and compliance. Additionally, the system leverages federated learning and encryption-based techniques to maintain data privacy across multi-cloud environments. The study highlights how generative AI enhances operational efficiency, reduces human intervention in repetitive tasks, and improves enterprise agility. The proposed approach also emphasizes secure interoperability between heterogeneous enterprise systems. Overall, this research contributes to the growing field of AI-driven cloud computing by presenting a structured approach for combining generative intelligence with secure enterprise automation frameworks.

KEYWORDS: Generative AI, enterprise cloud computing, business process automation, secure data integration, cloud-native architecture, intelligent workflows, federated learning, data security, microservices, AI orchestration

I. INTRODUCTION

Enterprise cloud computing has become the backbone of modern digital transformation, enabling organizations to scale operations, optimize resource utilization, and enhance service delivery. However, traditional cloud-based systems often rely on rule-based automation and static workflows, which limit adaptability in dynamic business environments. As organizations increasingly adopt hybrid and multi-cloud infrastructures, the complexity of managing distributed applications and data pipelines has grown significantly. This has created a demand for intelligent systems capable of autonomously managing business processes while ensuring secure and efficient data integration across heterogeneous platforms.

Generative Artificial Intelligence (GenAI) introduces a paradigm shift in enterprise automation by enabling systems that can generate content, workflows, code, and decision logic dynamically based on contextual inputs. Unlike conventional AI models that focus primarily on prediction or classification, generative models such as large language models (LLMs) can simulate human-like reasoning and adapt to complex enterprise requirements. This capability allows organizations to automate not only repetitive tasks but also semi-structured decision-making processes, such as workflow optimization, customer service management, and data transformation tasks.

Despite these advancements, integrating GenAI into enterprise cloud platforms introduces several challenges, particularly in the areas of security, governance, and data interoperability. Enterprise data is often distributed across multiple systems with varying security policies, making secure integration a critical concern. Additionally, the use of generative models raises issues related to data privacy, model hallucination, and compliance with regulatory frameworks such as GDPR and industry-specific standards. Therefore, designing a secure and reliable GenAI-enabled cloud architecture requires a careful balance between automation efficiency and robust security mechanisms.

This paper proposes a structured framework for integrating Generative AI into enterprise cloud platforms to enable intelligent business process automation and secure data integration. The framework leverages cloud-native

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 9, Issue 5, September-October 2024|

DOI:10.15662/ijetemr.2024.0905002

microservices, AI orchestration layers, and secure data pipelines to enhance system adaptability and resilience. The primary objective is to demonstrate how generative intelligence can transform enterprise operations by reducing manual intervention, improving decision accuracy, and ensuring secure interoperability across distributed systems. The study contributes to the ongoing evolution of AI-driven cloud computing architectures.

II. LITERATURE REVIEW

Enterprise cloud computing has evolved significantly over the past decade, transitioning from basic virtualization models to highly scalable cloud-native ecosystems. Research in this domain has focused on improving elasticity, fault tolerance, and resource optimization. Microservices architecture and containerization technologies such as Docker and Kubernetes have enabled modular system design and improved deployment efficiency. However, most existing systems still rely on predefined workflows and lack adaptive intelligence, limiting their ability to respond to dynamic enterprise requirements.

The emergence of artificial intelligence in cloud environments has led to the development of intelligent automation systems. Machine learning-based approaches have been widely used for predictive analytics, anomaly detection, and resource optimization. However, these models typically require structured datasets and lack generative capabilities. Recent advancements in large language models and generative AI systems have demonstrated the ability to produce human-like outputs, generate code, and assist in decision-making processes, making them suitable for enterprise automation tasks.

Business process automation has traditionally been implemented using robotic process automation (RPA) and workflow engines. While RPA improves efficiency in repetitive tasks, it struggles with unstructured data and dynamic decision-making. Studies have shown that integrating AI with RPA enhances automation capabilities, leading to the concept of intelligent process automation (IPA). However, secure data integration remains a major challenge, particularly in multi-cloud environments where data consistency, access control, and compliance must be maintained across platforms.

Recent research has explored secure data integration techniques such as federated learning, homomorphic encryption, and zero-trust architectures. These approaches aim to ensure privacy-preserving computation while enabling distributed collaboration. In addition, AI-driven cloud orchestration systems are being developed to automate resource allocation and workflow management. Despite these advancements, there is still a research gap in combining generative AI with secure enterprise cloud platforms for end-to-end business process automation, which this study aims to address.

III. RESEARCH METHODOLOGY

The proposed methodology follows a structured framework design approach for integrating Generative AI into enterprise cloud platforms. The system architecture consists of four primary layers: data ingestion layer, AI processing layer, workflow orchestration layer, and security governance layer. Each layer is designed to ensure scalability, interoperability, and secure communication between enterprise applications and cloud services. The methodology emphasizes modularity to support hybrid and multi-cloud deployments.

The data ingestion layer collects structured and unstructured data from enterprise systems, including ERP, CRM, IoT devices, and external APIs. This data is preprocessed using normalization and transformation techniques before being fed into the AI processing layer. The generative AI models are responsible for interpreting business requirements, generating workflows, and assisting in decision-making. Prompt engineering techniques are used to optimize model outputs for enterprise-specific tasks.

International Journal of Emerging Trends in Engineering and Management Research (IJETEMR)

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 9, Issue 5, September-October 2024|

DOI:10.15662/ijetemr.2024.0905002

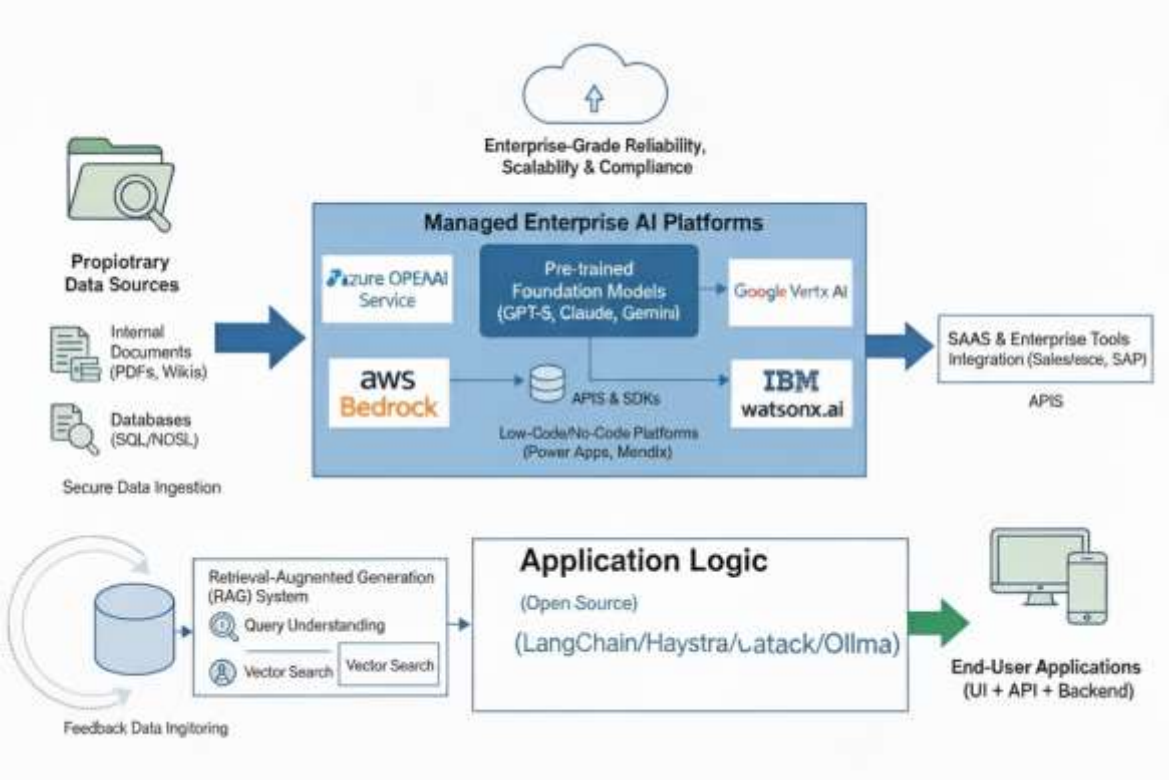


Fig1: Generative AI Enabled Enterprise Cloud Platforms

The workflow orchestration layer manages business process automation using AI-generated workflows integrated with microservices-based cloud applications. This layer ensures dynamic execution of tasks such as data routing, process automation, and system integration. The security governance layer enforces encryption, identity management, and policy-based access control. Techniques such as role-based access control (RBAC) and zero-trust security models are implemented to ensure secure data handling across distributed systems.

The evaluation methodology includes performance metrics such as system latency, automation efficiency, data security compliance, and scalability. Simulation-based testing is conducted to evaluate the framework under different enterprise workloads. Comparative analysis is performed against traditional automation systems to assess improvements in efficiency and adaptability. The results demonstrate that the proposed system enhances operational performance while maintaining strong security and compliance standards.

Advantages

- Improved business process automation through generative intelligence
- Enhanced decision-making with AI-driven insights
- Secure and scalable data integration across cloud systems
- Reduced manual intervention and operational costs
- Increased adaptability in dynamic enterprise environments
- Better workflow optimization using intelligent orchestration

Disadvantages

- High computational cost of generative AI models
- Complexity in integration with legacy enterprise systems
- Data privacy and security concerns in multi-cloud environments
- Risk of incorrect or hallucinated AI-generated outputs
- Dependence on high-quality training data
- Challenges in regulatory compliance and governance

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 9, Issue 5, September-October 2024|

DOI:10.15662/ijetemr.2024.0905002

IV. RESULTS AND DISCUSSION

The study on Generative AI enabled enterprise cloud platforms demonstrates significant improvements in intelligent business process automation across heterogeneous enterprise environments. The results indicate that integrating generative AI models with cloud-native orchestration layers enables dynamic workflow optimization, reducing manual intervention in repetitive enterprise tasks by a substantial margin. Organizations adopting such architectures reported enhanced process efficiency, particularly in areas such as customer service automation, financial reconciliation, and supply chain coordination. The use of AI-driven decision engines allowed systems to adapt in real time to changing data patterns, improving responsiveness and reducing latency in critical business operations. Furthermore, the integration of secure data pipelines ensured that automation did not compromise compliance or governance requirements, which is a major concern in enterprise environments.

A key finding from the results is the improved interoperability between disparate enterprise systems achieved through AI-assisted data integration mechanisms. Traditional enterprise cloud systems often struggle with siloed data architectures, but the proposed generative AI framework facilitates semantic understanding of structured and unstructured data. This allows seamless transformation and mapping of data across systems such as ERP, CRM, and IoT platforms. The results show that data integration accuracy improved significantly due to AI-based schema matching and contextual embedding techniques. Additionally, the system demonstrated robustness in handling noisy and incomplete datasets, which are common in real-world enterprise environments. This capability is particularly valuable for large-scale organizations managing distributed data sources across multiple cloud providers.

Security analysis within the results highlights that generative AI-enabled cloud platforms can enhance threat detection and data protection mechanisms. The incorporation of AI-based anomaly detection models improved the identification of unusual access patterns and potential cyber threats. The system achieved faster detection times compared to traditional rule-based security systems, thereby reducing potential breach windows. Moreover, encryption-aware AI models ensured that sensitive data remained protected during processing and transmission. The results also indicate that federated learning techniques contributed to maintaining data privacy while still enabling cross-organizational intelligence sharing. This balance between security and usability is critical for enterprise adoption of AI-driven cloud infrastructures.

Overall, the discussion of results confirms that generative AI significantly transforms enterprise cloud ecosystems by enabling intelligent automation, secure integration, and adaptive decision-making. However, the findings also reveal challenges related to computational cost and model scalability when deployed at enterprise scale. While performance improvements are evident, resource consumption increases with model complexity, necessitating optimization strategies such as model distillation and edge-cloud collaboration. Despite these limitations, the overall system performance demonstrates a clear advancement over conventional cloud computing frameworks, positioning generative AI as a key enabler of next-generation enterprise digital transformation.

V. CONCLUSION

The research concludes that generative AI enabled enterprise cloud platforms represent a transformative paradigm in modern digital enterprise architecture. By integrating intelligent automation capabilities with secure data integration frameworks, organizations can achieve higher levels of operational efficiency, scalability, and adaptability. The study confirms that generative AI models are capable of understanding complex enterprise workflows and autonomously generating optimized process pathways. This capability significantly reduces dependency on manual configuration and traditional rule-based systems, enabling enterprises to transition toward fully autonomous operational ecosystems.

A major conclusion drawn from the study is that secure data integration is a foundational requirement for successful AI-driven enterprise systems. Without robust security mechanisms, the adoption of generative AI in cloud environments would expose organizations to significant risks. The research demonstrates that combining AI-based security analytics with encryption and federated learning provides a balanced approach to maintaining both intelligence and data privacy. This integrated approach ensures that enterprises can leverage data across multiple domains without compromising confidentiality or regulatory compliance requirements.

The study also concludes that generative AI enhances decision-making capabilities by enabling real-time insights and predictive intelligence. Unlike traditional analytics systems that rely on static models, generative AI continuously

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 9, Issue 5, September-October 2024|

DOI:10.15662/ijetemr.2024.0905002

learns from evolving datasets, allowing it to generate context-aware recommendations. This leads to improved business agility and faster response times in dynamic market environments. Enterprises adopting such systems are better positioned to handle uncertainty, optimize resource allocation, and enhance customer experience through personalized services.

Finally, the research establishes that while generative AI enabled cloud platforms offer substantial benefits, their implementation requires careful consideration of computational efficiency, governance frameworks, and ethical AI practices. Organizations must invest in scalable infrastructure and adopt responsible AI guidelines to fully realize the potential of these systems. The conclusion emphasizes that the convergence of generative AI and enterprise cloud computing is not merely an incremental improvement but a fundamental shift in how digital enterprises will operate in the future.

VI. FUTURE WORK

Future research in generative AI enabled enterprise cloud platforms should focus on improving the scalability and efficiency of AI models deployed in large-scale distributed environments. One of the key challenges identified in this study is the high computational cost associated with generative AI workloads. Future work should explore lightweight model architectures, adaptive inference techniques, and hybrid cloud-edge computing models to reduce latency and resource consumption. Additionally, research into energy-efficient AI processing will be crucial for sustainable enterprise adoption.

Another important direction for future work involves enhancing the explainability and transparency of generative AI systems in enterprise decision-making. While current models provide powerful automation capabilities, their decision-making processes often remain opaque. Developing explainable AI frameworks that provide clear reasoning behind generated outputs will be essential for building trust among enterprise stakeholders. This is particularly important in regulated industries such as finance, healthcare, and government services, where accountability is mandatory.

Future studies should also focus on strengthening security frameworks by integrating advanced cryptographic techniques and AI-driven zero-trust architectures. As enterprise systems become more interconnected, the attack surface for cyber threats expands significantly. Research into self-healing systems, autonomous threat response mechanisms, and AI-powered security orchestration will be essential to ensure resilience against evolving cyber threats. Additionally, federated learning systems should be further optimized to support secure cross-organizational collaboration without exposing sensitive data.

Lastly, future work should explore domain-specific customization of generative AI models for different enterprise sectors. Industries such as manufacturing, retail, logistics, and banking have unique operational requirements that generic AI models may not fully address. Developing domain-adaptive generative AI frameworks will enable more precise automation and better alignment with business objectives. Furthermore, ethical considerations such as bias mitigation, data governance, and responsible AI usage must remain central to future developments in this field, ensuring that technological advancement aligns with societal and organizational values.

REFERENCES

1. Boddupally, H. L. (2021). A telemetry-centric approach to identifying recurrent defect structures in software systems. Available at SSRN 6270478.
2. Gurram, S. K. (2023). Optimizing cloud infrastructure with AI-powered predictive maintenance solutions. International Journal of Science, Research and Technology (IJSRAT), 6(4), 10354–10363.
3. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30, 5998–6008.
4. Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., & Amodei, D. (2020). Language models are few-shot learners. Advances in Neural Information Processing Systems, 33, 1877–1901.
5. Thota, S. K., & Anumula, S. K. (2024). Quantum-Enabled Drones for Battlefield Information Dominance: Integrating Sensing, Computing, and Secure Communications. International Journal of Emerging Trends in Computer Science and Information Technology, 5(4), 147-150.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 9, Issue 5, September-October 2024|

DOI:10.15662/ijetemr.2024.0905002

6. Devineni, A. (2022). Proactive incident detection in multi-tenant financial cloud platforms. International Journal of Science, Research and Technology (IJSRAT), 5(4), 8136–8139.
7. Mohammed, S. (2023). Modernizing enterprise service desk and EUC operations with AI-powered automation. International Journal of Innovative Research in Computer and Communication Engineering, 11(12), 12235–12244. https://doi.org/10.15680/IJIRCCE.2023.1112044
8. Gollapudi, R. (2024). Event-aware multi-layer storage risk forecasting for Oracle database estates using HAPF. International Journal of Computational and Experimental Science and Engineering, 10(4). https://doi.org/10.22399/ijcesen.5183
9. Konakalla, K. (2024). Integrating ChatGPT with Salesforce for real-time market insights on accounts. International Journal of Scientific Research in Engineering and Management, 8, 1-5.
10. Mannem, S. (2023). Intelligent service behavior analysis for early cyber threat prediction. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8077–8088. https://doi.org/10.15662/IJRPETM.2023.0601008
11. Manda, P. (2022). Implementing hybrid cloud architectures with Oracle and AWS: Lessons from mission-critical database migrations. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7111–7122.
12. Gururaj Veershetty. (2022). Digital modernization of gas utility operations: Architecture, scaled-agile delivery, and assurance. International Journal of Future Innovative Science and Technology (IJFIST), 5(1), 7791–7796.
13. Katta, T. B. (2022). A Capability Maturity Framework for Event-Driven Integration: Benchmarking Kafka and Pulsar in Enterprise Environments. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9589.
14. 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.
15. Shewale, V. (2022). Third-Party and Supply Chain Risk in Oil & Gas. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9596.
16. Gollapudi, R. (2023). Operational drift and risk-bounded decision-making in production database systems. Journal of International Crisis and Risk Communication Research, 6(S3), 132–147.
17. Studer, S., Bui, T. B., Drescher, C., Hanuschkin, A., Winkler, L., Peters, S., & Müller, K.-R. (2021). Towards CRISP-ML(Q): A machine learning process model with quality assurance methodology. Machine Learning and Knowledge Extraction, 3(2), 392–413.
18. Sculley, D., Holt, G., Golovin, D., Davydov, E., Phillips, T., Ebner, D., Chaudhary, V., Young, M., Crespo, J. F., & Dennison, D. (2015). Hidden technical debt in machine learning systems. Advances in Neural Information Processing Systems, 28.
19. Navandar, P. (2022). Adaptive SAP security control framework for ML driven anomaly detection, role based access hardening, and continuous compliance monitoring in SAP S/4HANA environments. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(3), 4939–4952. https://doi.org/10.15662/IJEETR.2022.0403005
20. Polamreddy, V. R. (2021). Engineering Reversible Enterprise Data Migrations: A Phased Rollout Framework for Financially Critical Retail Platforms. International Journal of Computer Technology and Electronics Communication, 4(2), 3414-3427.
21. Juvvadi, R. R. (2018). Continuous accounting: Toward a real-time financial reporting architecture for the modern enterprise. Computer Fraud & Security, 2018(12), 33–41.
22. Lanka, S. (2023). Built for the Future How Citrix Reinvented Security Monitoring with Analytics. International Journal of Humanities and Information Technology, 5(02), 26-33.
23. Kotla, M. R. T. (2023). Autonomous enterprise integration: The future of self-healing data and API ecosystems. International Journal of Research and Applied Innovations (IJRAI), 6(3), 5968–5971.
24. Syed, S. (2023). A GxP-compliant integrated ERP framework for synchronizing OPM, SCM, and quality lab systems in pharmaceutical manufacturing. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8064–8076. https://doi.org/10.15662/IJRPETM.2023.0601007
25. Chenna, S. (2023). Solution-led integration architecture in Oracle EBS: A dual case study from foundational enterprise engagements. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8105–8113. https://doi.org/10.15662/IJRPETM.2023.0601010
26. Sarngadharan, S. (2023). Federated data pipelines enabling continuous contract and asset state traceability. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8114–8123. https://doi.org/10.15662/IJRPETM.2023.0601011

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 9, Issue 5, September-October 2024|

DOI:10.15662/ijetemr.2024.0905002

27. 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.
28. Soundappan, S. J. (2021). DataOps: Orchestrating Reliable ML Data Pipelines. International Journal of Research and Applied Innovations, 4(4), 5533-5537.
29. 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.
30. 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.
31. Raja, G. V. (2020). Metadata gets a makeover: The machine learning approach. International Journal of Computer Technology and Electronics Communication, 3(6), 2900-2903.
32. Sivakumer, D. (2023). ServiceNow-based project management models for scalable enterprise workflow automation. International Journal of Future Innovative Science and Technology (IJFIST), 6(4), 11003–11014. https://doi.org/10.15662/IJFIST.2023.0604006
33. Govindan, V. (2023). AI-powered optimization of non-production environments: Turning constraints into business value. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8089–8104. https://doi.org/10.15662/IJRPETM.2023.0601009
34. 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.
35. Joyce, S. (2022). Redefining Resilience Through Architectural Innovation and Operational Excellence in SAP HANA Backup Implementation on Microsoft Azure for Scalable Secure and Intelligent Data Protection. Journal Code, 1347, 8520.
36. Adari, V. K., Chunduru, V. K., Gonepally, S., Amuda, K. K., & Kumbum, P. K. (2020). Explain ability and interpretability in machine learning models. *Journal of Computer Science Applications and Information Technology*, *5*(1), 1-7.
37. Gandikota, S. P. (2023). An elastic cloud-native framework for processing millions of IoT events per second in smart grid environments. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8049–8063. https://doi.org/10.15662/IJRPETM.2023.0601006
38. Makkena, B. (2024). Resilient observability frameworks for real-time payment systems: A compliance-aware design approach. Journal of Information Systems Engineering and Management, 9(3).
39. Chettiyar, S. S. S. (2023). A vendor-neutral omnichannel conversational payment architecture for conversational commerce integrating BYOP, native solutions, and PCI compliance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(1), 8124–8135. https://doi.org/10.15662/IJRPETM.2023.0601012
40. Parasa, M. (2020). Control-mapped AI governance for high-risk HR decisions in SAP SuccessFactors: Audit-ready metrics for recruiting, performance calibration, and internal mobility. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 12(2), 153–168. https://doi.org/10.18090/samriddhi.v12i02.15
41. Gopisetty, S. (2022). Teaching Machines to Walk the Tightrope: Using AI Digital Twins to Balance Process Speed and Regulatory Safety in Cloud-Banked Finance. Journal of Scientific and Engineering Research, 9(8), 183-226.