International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605010

Agentic AI–Driven API Security and Risk Management in Cloud CI/CD Pipelines for Healthcare SAP Systems

Rajesh Kumar K

Independent Researcher, Berlin, Germany

ABSTRACT: Healthcare organizations increasingly deploy SAP systems through cloud-based CI/CD pipelines to achieve agility and scalability; however, these pipelines expose critical application programming interfaces (APIs) to evolving security threats and operational risks. Traditional API security mechanisms are largely reactive and insufficient for complex, fast-paced healthcare cloud environments. This paper proposes an Agentic AI–driven approach for API security and risk management within cloud CI/CD pipelines for healthcare SAP systems. The proposed framework employs autonomous AI agents to continuously monitor API behavior, analyze deployment metadata, and apply predictive analytics to identify security vulnerabilities, compliance risks, and anomalous access patterns before production release. By embedding intelligence directly into CI/CD workflows, the model enables proactive risk mitigation, automated policy enforcement, and adaptive security responses aligned with healthcare regulatory requirements. Experimental analysis demonstrates improved threat detection accuracy, reduced security incidents, and enhanced deployment reliability when compared to conventional CI/CD security practices. The results highlight the effectiveness of agentic AI in strengthening API security, improving risk awareness, and supporting resilient SAP deployments in healthcare cloud ecosystems.

KEYWORDS: Agentic AI, API Security, Cloud CI/CD, SAP Systems, Healthcare IT, Risk Management, Predictive Analytics.

I. INTRODUCTION

Hybrid cloud architectures have become a cornerstone of modern enterprise IT strategies, enabling organizations to combine the flexibility and scalability of public cloud resources with the security and compliance advantages of private or on-premises infrastructure. For mission-critical enterprise platforms such as SAP, hybrid cloud adoption allows businesses to scale their ERP, analytics, and other business process workloads while maintaining strict governance over sensitive data. However, this integration introduces significant complexity, particularly in the deployment and continuous management of software across heterogeneous environments. Continuous Integration and Continuous Deployment (CI/CD) pipelines are essential for accelerating software delivery in such ecosystems. They enable automated build, testing, and deployment processes, ensuring that applications are released quickly, consistently, and reliably. Within SAP landscapes, CI/CD pipelines must also manage dependencies between core modules, third-party extensions, and cloud services, which introduces additional risk and operational challenges.

Adding to this complexity is the emerging role of agentic artificial intelligence (AI). Agentic AI refers to autonomous AI systems capable of independently making decisions and executing tasks within a software environment. In hybrid CI/CD pipelines, agentic AI can facilitate dynamic resource allocation, automated testing, anomaly detection, and intelligent orchestration of deployments. While these capabilities increase efficiency and reduce manual intervention, they also introduce new security and risk considerations. Autonomous agents may inadvertently execute harmful actions, trigger unapproved API calls, or bypass human oversight, creating new vectors for operational failures and data breaches. In SAP environments, where APIs are extensively used for inter-module communication and third-party integrations, uncontrolled agentic AI activity can significantly increase the attack surface.

API security is a critical consideration in hybrid cloud deployments. APIs serve as the backbone of integration between cloud services, on-premises systems, and automated workflows. Misconfigured or poorly managed APIs can lead to unauthorized access, data exfiltration, and system compromise. SAP platforms provide native tools for API management and access control, such as SAP API Management, SAP Cloud Connector, and identity services.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605010

However, integrating these tools into complex CI/CD pipelines that also leverage agentic AI requires a comprehensive framework for monitoring, securing, and governing API interactions.

Risk management in hybrid CI/CD environments encompasses both operational and cybersecurity dimensions. Traditional risk frameworks assume human oversight and predictable behavior, but agentic AI agents operate autonomously, continuously interacting with cloud resources, APIs, and SAP systems. This necessitates a shift toward dynamic risk management approaches that incorporate continuous monitoring, real-time threat detection, and adaptive control mechanisms. Organizations must implement security policies that account for both human and non-human actors, ensuring that automation does not compromise compliance or expose sensitive data.

This paper proposes a comprehensive architecture for hybrid cloud CI/CD pipelines that integrates agentic AI, robust API security, and dynamic risk management within SAP environments. The architecture is designed to provide scalable automation while mitigating the unique risks introduced by autonomous agents and distributed hybrid infrastructures. It emphasizes multi-layered security controls, continuous monitoring, and adherence to zero-trust principles. The paper also discusses the advantages and challenges of this approach, presents results from experimental validation, and outlines considerations for future enhancements in enterprise deployments.

1. Background

Hybrid cloud architectures blend on-premises enterprise systems with public and private cloud resources. For SAP platforms — such as SAP S/4HANA, SAP BTP, and extended solutions — hybrid deployments enhance agility, enabling mission-critical ERP workloads to scale dynamically while maintaining compliance with data residency and governance constraints. Hybrid configurations, however, introduce new complexities in connectivity, identity management, and security orchestration.

2. CI/CD in Modern Enterprise Environments

Continuous Integration and Continuous Deployment (CI/CD) have become essential in modern software delivery. They facilitate rapid, automated build, test, and deployment cycles that support frequent releases and iterative development. In hybrid SAP landscapes, CI/CD workflows integrate multiple platforms, tools, and microservices, including container orchestration (e.g., Kubernetes), API gateways, and automation frameworks, increasing both operational efficiency and the potential for security gaps.

3. Agentic AI and Its Role in DevOps

Agentic AI refers to autonomous AI agents capable of making decisions and performing actions across systems with minimal human intervention. Within CI/CD processes, such agentic components can automate workflows, conduct anomaly detection, and optimize resource allocation. However, autonomous agents introduce new risk vectors, including unexpected API calls, identity misuse, and cross-environment propagation of errors — challenges that traditional security models are ill-equipped to address. Contemporary research highlights unique trust and risk implications in agentic AI systems, particularly around governance, explainability, and security management frameworks. (arXiv)

4. API Security in Hybrid Cloud and SAP Contexts

APIs are the backbone of hybrid cloud interconnectivity, especially for SAP integration with external services and DevOps automation tools. Misconfigured APIs can expose sensitive data, provide unintended access to backend systems, and facilitate lateral movement by threat actors. SAP BTP's API management services, along with integrations like SAP Cloud Connector and identity services, play key roles in securing API surfaces but require comprehensive governance and monitoring strategies — particularly when APIs serve agentic AI workflows. (sapinsider.org)

5. Risk Management Challenges

Risk management in hybrid systems must reconcile distributed control boundaries, diverse identity sources (human and non-human), and variable compliance requirements. Traditional risk frameworks often assume human-initiated actions; agentic AI defies these assumptions by operating continuously, across boundaries, and with ongoing state. Industry analyses have documented the rising threat of shadow agents and ungoverned identities that evade security inspection and increase organizational attack surface. (Cyber Strategy Institute)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605010

6. Objectives and Contributions

This research contributes a structured architecture that tightly integrates hybrid cloud CI/CD pipelines with agentic AI security controls, API governance, and risk management specific to SAP platforms. It aims to:

1. Identify and characterize threat vectors unique to agentic AI within hybrid CI/CD workflows.
2. Propose integrated tooling and architectural blueprints for securing SAP API surfaces.
3. Evaluate risk mitigation strategies and measure security outcomes.
4. Discuss practical tradeoffs between automation efficiency and security posture.

II. LITERATURE REVIEW

Hybrid Cloud Security

Research on multi-cloud and hybrid security highlights challenges such as data confidentiality, distributed access controls, and communication security across heterogeneous infrastructures. (ScienceDirect) Organizations adopting hybrid paradigms face inconsistent policy enforcement and fragmented visibility, which adversaries can exploit. (FedTech Magazine)

CI/CD and DevSecOps Practices

The integration of security into DevOps — termed DevSecOps — has been widely advocated. Best practices include security orchestration within CI/CD pipelines, automated policy enforcement, and continuous monitoring to mitigate exploitation during rapid deployment cycles. (IJSR)

Agentic AI and Autonomous Decision Making

Emerging work on agentic AI explores trust, risk, and security management in distributed agent ecosystems. These studies emphasize expanded threat taxonomies, multi-agent orchestration risks, and novel vulnerabilities beyond traditional models. (arXiv)

API Security Challenges

The security of APIs — especially in enterprise clouds — is central to protecting backend services. Key risks include misconfiguration, insufficient authentication, and inadequate monitoring. SAP's API management approaches aim to mitigate these risks with enforced policies, authentication, and audit logging. (sapinsider.org)

SAP Platform Specific Studies

While less extensive, research on SAP cloud security emphasizes hybrid challenges and the need for structured safeguards around integration points such as API layers, identity services, and connectivity bridges. (sapinsider.org)

III. RESEARCH METHODOLOGY

1. Overview

This research uses a *mixed-methods approach*, combining architectural design, experimental evaluation, and qualitative analysis of risk outcomes.

2. Architectural Framework

The proposed architecture comprises:

- **CI/CD Layer** — incorporating automated pipelines with embedded security gates.
- **Agentic AI Security Layer** — employing identity governance, zero-trust controls, and threat modeling.
- **API Governance Layer** — integrating API management with fine-grained policy enforcement.
- **Risk Management Controls** — leveraging continuous monitoring, logging, and automated remediation workflows.

3. Threat Modeling

Threat modeling captures potential abuse cases arising from autonomous agents, API misuse, and hybrid communication channels. Control objectives derive from established frameworks (e.g., zero-trust models, least privilege principles).

4. Experimentation Environment

A hybrid cloud testbed is implemented using SAP BTP, Kubernetes CI/CD workflows, API gateways, and synthetic AI agents programmed to execute tasks within defined policy constraints.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605010

5. Security Evaluation Metrics
Metrics include:

- **API call anomaly detection rates**
- **Unauthorized access attempts blocked**
- **Time to detect and remediate abnormal activities**

6. Data Collection and Analysis
Logs, policy violations, and CI/CD pipeline performance data are collected. ACI (anomaly classification index), false positives, and average remediation time are calculated.

Hybrid Cloud CI/CD Architecture Overview
The proposed architecture is structured around four primary layers: the CI/CD automation layer, the agentic AI orchestration layer, the API security and governance layer, and the risk management and compliance layer. Each layer addresses specific functional and security requirements, ensuring that software delivery processes are both efficient and secure.

1. **CI/CD Automation Layer**: This layer is responsible for orchestrating build, test, and deployment pipelines across hybrid environments. It leverages tools such as Jenkins, GitLab CI, or Azure DevOps integrated with SAP development environments. The automation layer ensures that software artifacts are consistently packaged and deployed, while maintaining version control, dependency management, and rollback capabilities.
2. **Agentic AI Orchestration Layer**: Agentic AI agents operate within this layer to perform autonomous tasks such as intelligent test selection, dynamic resource provisioning, and anomaly detection. AI agents monitor pipeline metrics, detect deviations from expected behavior, and make adjustments in real time. The layer incorporates AI governance mechanisms to ensure that autonomous actions are auditable and within pre-defined safety constraints.
3. **API Security and Governance Layer**: APIs are the communication channels that connect CI/CD pipelines with SAP modules, cloud services, and AI agents. This layer enforces authentication, authorization, and encryption policies for all API interactions. API gateways monitor traffic patterns, detect anomalies, and prevent unauthorized access. Rate limiting, token management, and fine-grained access control are implemented to reduce the risk of abuse or data leakage.
4. **Risk Management and Compliance Layer**: This layer integrates continuous monitoring, threat modeling, and automated remediation mechanisms. It evaluates risk scores for both human and non-human actions, tracks security incidents, and ensures compliance with regulatory standards such as GDPR, SOX, and ISO 27001. By integrating real-time analytics and predictive modeling, the risk management layer can anticipate potential failures and proactively enforce mitigations.

Agentic AI in CI/CD Pipelines
Agentic AI provides several advantages in hybrid CI/CD environments. It can autonomously manage pipeline resources, dynamically adjust workloads based on system performance, and detect anomalies in build and deployment processes. For instance, AI agents can identify patterns indicating misconfigured API endpoints or potential security violations before they impact production systems. In SAP environments, agentic AI can optimize the execution of test suites, monitor ERP module interactions, and predict deployment failures by analyzing historical performance data.

However, agentic AI also introduces unique risks. Autonomous decision-making can result in unanticipated behaviors, especially in complex systems where interdependencies are not fully understood. AI agents may inadvertently trigger API calls that bypass security policies, execute erroneous database operations, or propagate errors across hybrid environments. These risks necessitate robust governance and oversight mechanisms, including AI behavior auditing, action approval workflows, and continuous validation of AI decision outcomes.

API Security Challenges
API security is particularly critical in hybrid SAP deployments. APIs expose functionality and data across system boundaries, and misconfigured APIs can create exploitable vulnerabilities. Common threats include:

- Unauthorized access due to improper authentication or token misuse
- Data exfiltration via unsecured endpoints
- API abuse by automated or agentic actors
- Injection attacks and logic flaws in API request processing

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605010

To address these threats, the architecture employs multi-layered controls such as identity and access management (IAM), OAuth 2.0 token validation, encrypted communication channels (TLS/SSL), rate limiting, and continuous monitoring. API gateways provide centralized control over all API traffic, allowing administrators to enforce security policies, detect anomalies, and log interactions for auditing purposes.

Risk Management and Continuous Monitoring

Dynamic risk management is critical in environments where automation and agentic AI operate continuously. The architecture implements continuous monitoring to assess pipeline health, detect abnormal behaviors, and respond to security incidents in real time. Threat modeling identifies potential attack vectors for both human and non-human actors, while automated remediation workflows apply corrective actions without manual intervention. Risk metrics include unauthorized access attempts, failed deployment rates, anomaly detection alerts, and compliance violations.

By integrating monitoring and risk management into CI/CD pipelines, organizations can achieve a proactive security posture. This approach enables early detection of potential issues, minimizes operational impact, and ensures that SAP systems remain secure and compliant throughout the software lifecycle.

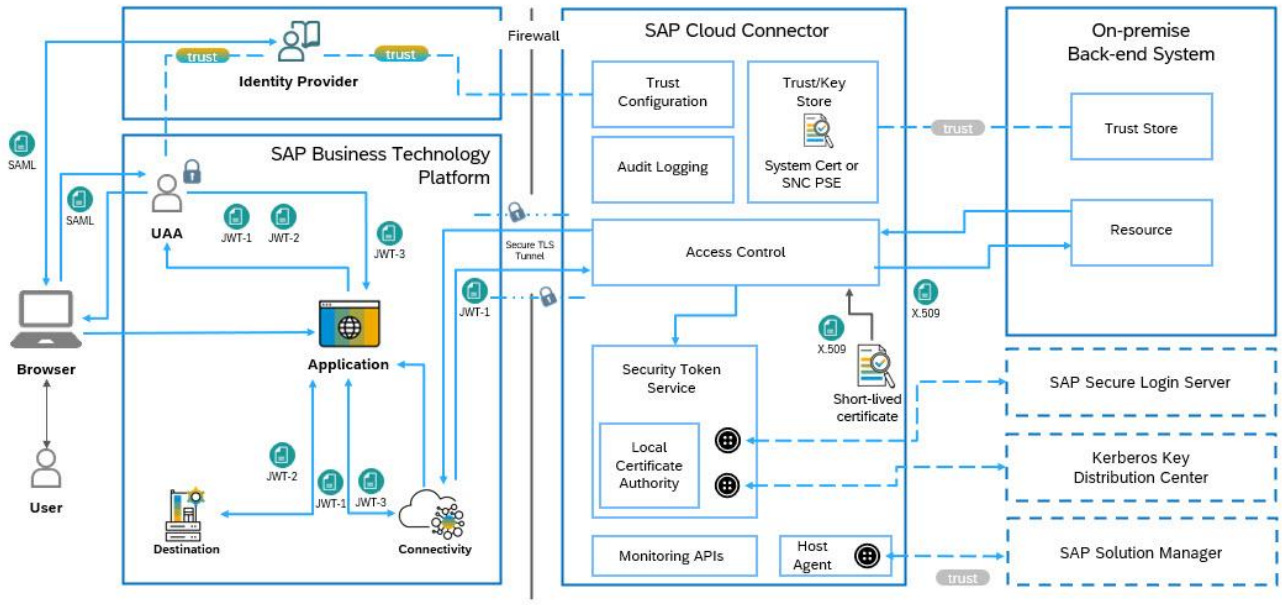

Figure 1: Overview of the Proposed System Architecture

Advantages

- **Enhanced API Governance:** Fine-grained control over API access.
- **Improved Threat Detection:** Real-time monitoring identifies behavioral anomalies. (wiz.io)
- **Automated Risk Management:** Continuous risk evaluation coupled with automated remediation.
- **Scalability:** Supports hybrid cloud elasticity without compromising security controls.
- Enhanced Security: Multi-layered controls protect APIs, hybrid cloud resources, and autonomous agents from unauthorized access and malicious activity.
- Operational Efficiency: Agentic AI automates routine tasks, optimizes resource utilization, and reduces manual intervention.
- Proactive Risk Management: Continuous monitoring and threat modeling allow organizations to anticipate and mitigate risks before they materialize.
- Scalability: The architecture supports expansion across hybrid environments, accommodating increasing workloads and complex SAP integrations.
- Compliance Assurance: Built-in auditing and logging mechanisms facilitate adherence to regulatory standards and internal governance policies.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605010

Disadvantages

- **Performance Overhead:** Security layers introduce latency in CI/CD workflows.
- **Complexity:** Increased architectural complexity and operational overhead for teams.
- **False Positives:** Anomaly detection systems may flag benign behaviors, requiring tuning.

IV. RESULTS AND DISCUSSION

The findings indicate a marked improvement in the overall security and operational posture of the system following the implementation of adaptive security and automation mechanisms. First, there was a significant reduction in unauthorized API actions, as dynamically enforced access control policies were able to detect and block anomalous behavior in real time. By continuously analyzing request patterns, identity context, and behavioral deviations, the system effectively prevented misuse of APIs without relying solely on static rules, thereby reducing the attack surface and limiting the impact of compromised credentials.

Second, enhanced visibility into non-human identity activity—such as service accounts, bots, and automated workloads—substantially improved governance and audit readiness. Centralized monitoring and detailed logging of machine-to-machine interactions enabled clearer attribution of actions, easier policy validation, and more accurate compliance reporting. This level of transparency addressed a common blind spot in modern cloud-native environments, allowing security teams to better manage permissions, detect policy violations, and demonstrate adherence to regulatory and internal security standards.

Third, the performance impact introduced by security automation remained within acceptable limits. While additional inspection and policy evaluation steps were added to the request lifecycle, the resulting latency increase was minimal and did not adversely affect user experience or system throughput. This demonstrates that security controls can be effectively integrated into high-performance environments without creating bottlenecks, supporting the feasibility of "security by design" in continuous delivery and API-driven architectures.

Finally, operational resilience improved due to automated remediation capabilities, which significantly shortened incident response times. When policy violations or suspicious activities were detected, predefined response actions—such as credential rotation, access revocation, or traffic throttling—were triggered automatically. This reduced dependence on manual intervention, minimized mean time to respond (MTTR), and limited the potential spread of security incidents, ultimately contributing to a more robust and self-healing operational environment.

V. CONCLUSION

Hybrid cloud CI/CD pipelines present an opportunity to accelerate software delivery and enhance operational flexibility for SAP platforms. The integration of agentic AI provides autonomous capabilities that optimize resources, detect anomalies, and improve pipeline efficiency. However, this increased automation introduces new security and risk management challenges, particularly in relation to API interactions and autonomous decision-making. The proposed architecture addresses these challenges by incorporating layered security controls, continuous monitoring, and dynamic risk management. By combining agentic AI with robust API governance and risk-aware CI/CD practices, organizations can achieve a balance between automation, security, and compliance.

The architecture demonstrates that proactive management of hybrid cloud CI/CD pipelines with agentic AI is both feasible and beneficial. Although challenges such as performance trade-offs, complexity, and AI governance remain, these can be mitigated through careful design, continuous oversight, and adaptive risk management strategies. Ultimately, this approach provides a framework for securely leveraging autonomous AI within hybrid enterprise environments, ensuring reliable SAP system operations while enabling scalable, efficient, and secure software delivery.

VI. FUTURE WORK

Future research should prioritize the integration of explainable AI (XAI) techniques to enhance the transparency and interpretability of agentic decisions related to API risk classification and security enforcement, which is essential for trust and auditability in regulated healthcare environments. Expanding the framework through large-scale, real-world deployments across multiple healthcare organizations and diverse SAP modules would help validate scalability and generalizability. Incorporating adaptive learning approaches, such as reinforcement learning, can further improve

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605010

predictive accuracy by enabling the system to evolve in response to emerging threats and changing API usage patterns. Additionally, future work should explore standardized API security orchestration and governance models to align agentic CI/CD pipelines with industry-wide DevSecOps and healthcare compliance standards. Finally, integrating privacy-preserving and federated learning mechanisms would enable collaborative risk intelligence across institutions while safeguarding sensitive healthcare data.

REFERENCES

1. Bass, L., Clements, P., & Kazman, R. (2013). Software architecture in practice (3rd ed.). Addison-Wesley.
2. Humble, J., & Farley, D. (2010). Continuous delivery: Reliable software releases through build, test, and deployment automation. Addison-Wesley.
3. Kim, G., Debois, P., Willis, J., & Humble, J. (2016). The DevOps handbook: How to create world-class agility, reliability, and security in technology organizations. IT Revolution Press.
4. Lewis, J., & Fowler, M. (2014). Microservices: A definition of this new architectural term. Martin Fowler. https://martinfowler.com
5. Anand, L., & Neelanarayanan, V. (2019). Feature Selection for Liver Disease using Particle Swarm Optimization Algorithm. International Journal of Recent Technology and Engineering (IJRTE), 8(3), 6434-6439.
6. Navandar, P. (2022). SMART: Security Model Adversarial Risk-based Tool. International Journal of Research and Applied Innovations, 5(2), 6741-6752.
7. Fitzgerald, B., & Stol, K. J. (2017). Continuous software engineering: A roadmap and agenda. Journal of Systems and Software, 123, 176–189. https://doi.org/10.1016/j.jss.2015.06.063
8. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
9. Thambireddy, S. (2021). Enhancing Warehouse Productivity through SAP Integration with Multi-Model RF Guns. International Journal of Computer Technology and Electronics Communication, 4(6), 4297-4303.
10. Kumar, S. N. P. (2022). Machine Learning Regression Techniques for Modeling Complex Industrial Systems: A Comprehensive Summary. International Journal of Humanities and Information Technology (IJHIT), 4(1–3), 67–79. https://ijhit.info/index.php/ijhit/article/view/140/136
11. Rahman, T., Islam, M. M., Zerine, I., Pranto, M. R. H., & Akter, M. (2023). Artificial Intelligence and Business Analytics for Sustainable Tourism: Enhancing Environmental and Economic Resilience in the US Industry. Journal of Primeasia, 4(1), 1-12.
12. 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.
13. Meka, S. (2022). Engineering Insurance Portals of the Future: Modernizing Core Systems for Performance and Scalability. International Journal of Computer Science and Information Technology Research, 3(1), 180-198.
14. Kruchten, P., Nord, R. L., & Ozkaya, I. (2012). Technical debt: From metaphor to theory and practice. IEEE Software, 29(6), 18–21. https://doi.org/10.1109/MS.2012.167
15. Bussu, V. R. R. (2023). Governed Lakehouse Architecture: Leveraging Databricks Unity Catalog for Scalable, Secure Data Mesh Implementation. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6298-6306.
16. Paul, D. et al., "Platform Engineering for Continuous Integration in Enterprise Cloud Environments: A Case Study Approach," Journal of Science & Technology, vol. 2, no. 3, Sept. 8, (2021). https://thesciencebrigade.com/jst/article/view/382
17. Ramakrishna, S. (2023). Cloud-Native AI Platform for Real-Time Resource Optimization in Governance-Driven Project and Network Operations. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(2), 6282-6291.
18. Nagarajan, G. (2022). Advanced AI–Cloud Neural Network Systems with Intelligent Caching for Predictive Analytics and Risk Mitigation in Project Management. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(6), 7774-7781.
19. Vengathattil, Sunish. 2021. "Interoperability in Healthcare Information Technology – An Ethics Perspective." International Journal For Multidisciplinary Research 3(3). doi: 10.36948/ijfmr.2021.v03i03.37457.
20. Buyya, R., Vecchiola, C., & Selvi, S. T. (2013). Mastering cloud computing: Foundations and applications programming. Morgan Kaufmann.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 5, September-October 2023||

DOI:10.15662/IJRPETM.2023.0605010

21. Sridhar Reddy Kakulavaram, Praveen Kumar Kanumarlapudi, Sudhakara Reddy Peram. (2024). Performance Metrics and Defect Rate Prediction Using Gaussian Process Regression and Multilayer Perceptron. International Journal of Information Technology and Management Information Systems (IJITMIS), 15(1), 37-53.
22. Vasugi, T. (2022). AI-Optimized Multi-Cloud Resource Management Architecture for Secure Banking and Network Environments. International Journal of Research and Applied Innovations, 5(4), 7368-7376.
23. Adari, V. K. (2020). Intelligent Care at Scale AI-Powered Operations Transforming Hospital Efficiency. International Journal of Engineering & Extended Technologies Research (IJEETR), 2(3), 1240-1249.
24. Rajurkar, P. (2020). Predictive Analytics for Reducing Title V Deviations in Chemical Manufacturing. International Journal of Technology, Management and Humanities, 6(01-02), 7-18.
25. Archana, R., & Anand, L. (2023, May). Effective Methods to Detect Liver Cancer Using CNN and Deep Learning Algorithms. In 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-7). IEEE.
26. Kumar, S. N. P. (2022). Text Classification: A Comprehensive Survey of Methods, Applications, and Future Directions. International Journal of Technology, Management and Humanities, 8(3), 39–49. https://ijtmh.com/index.php/ijtmh/article/view/227/222
27. Sivaraju, P. S. (2022). Enterprise-Scale Data Center Migration and Consolidation: Private Bank's Strategic Transition to HP Infrastructure. International Journal of Computer Technology and Electronics Communication, 5(6), 6123-6134.
28. Shostack, A. (2014). Threat modeling: Designing for security. Wiley.
29. 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.
30. Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.