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 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703015

Unified Artificial Intelligence Architecture for Enterprise Systems Combining Secure Cloud Computing SAP and Agentic AI

Leslie Teo

AI Product Architect, AI Singapore, Singapore

ABSTRACT: Unified Artificial Intelligence (AI) architectures are emerging as a foundational approach for next-generation enterprise systems that integrate secure cloud computing, SAP enterprise platforms, and agentic AI capabilities. As organizations increasingly rely on distributed digital ecosystems, there is a growing need for architectures that unify data, intelligence, and autonomous decision-making within a secure and scalable environment. Agentic AI introduces autonomous reasoning, planning, and execution capabilities that go beyond traditional predictive analytics, enabling systems to independently perform complex enterprise tasks. When combined with SAP's enterprise resource planning infrastructure and secure cloud computing environments, these capabilities enable end-to-end intelligent automation across business functions such as finance, supply chain, human resources, and customer operations. However, such integration introduces challenges related to governance, security, interoperability, and ethical AI deployment. This paper proposes a unified AI architecture that integrates secure cloud infrastructure, SAP enterprise systems, and agentic AI models into a cohesive framework. The architecture emphasizes data security, zero-trust principles, explainability, and scalable AI orchestration. The study highlights how this unified approach improves operational efficiency, decision intelligence, and enterprise resilience while ensuring compliance and cybersecurity in modern digital ecosystems.

KEYWORDS: Agentic AI, Unified AI Architecture, SAP Integration, Secure Cloud Computing, Enterprise Systems, Autonomous AI, Intelligent Automation, Zero Trust Security, Enterprise Architecture, AI Governance

I. INTRODUCTION

The evolution of enterprise systems has entered a new phase driven by artificial intelligence, cloud computing, and autonomous decision-making technologies. Traditional enterprise architectures were primarily designed around centralized databases and rule-based workflows, which limited scalability and adaptability in dynamic business environments. With the emergence of secure cloud computing platforms and advanced AI models, enterprises are now transitioning toward intelligent ecosystems capable of real-time reasoning and autonomous operations. SAP, as a leading enterprise resource planning (ERP) system, plays a central role in this transformation by integrating core business processes across finance, logistics, human resources, and supply chain management. The introduction of agentic AI, which enables systems to perform goal-oriented reasoning and autonomous task execution, further enhances the capabilities of enterprise platforms. This convergence of SAP systems, cloud computing, and agentic AI forms the foundation for a unified artificial intelligence architecture.

Secure cloud computing provides the essential infrastructure for deploying large-scale AI-driven enterprise systems. It enables elastic scalability, distributed processing, and global accessibility of enterprise applications. However, as enterprises migrate critical workloads to the cloud, concerns regarding cybersecurity, data privacy, and system integrity become increasingly important. Zero-trust architectures, encryption protocols, identity and access management systems, and secure API gateways are essential components of modern enterprise security frameworks. When integrated with SAP systems, cloud computing allows organizations to unify their data sources and business processes while maintaining high levels of security and compliance. The addition of AI capabilities introduces new dimensions of complexity, requiring robust governance frameworks to manage model behavior, data usage, and system accountability.

Agentic AI represents a significant advancement beyond traditional machine learning and predictive analytics systems. Unlike conventional AI models that only provide recommendations or predictions, agentic AI systems are capable of autonomous decision-making, planning, and execution of multi-step tasks. In enterprise environments, this means that AI agents can independently manage workflows such as procurement approvals, financial reconciliation, and customer service operations. When integrated with SAP systems, agentic AI can interact directly with enterprise modules to

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

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703015

execute business processes in real time. However, this autonomy raises critical concerns related to control, transparency, and ethical decision-making. Ensuring that agentic AI systems operate within defined boundaries and comply with enterprise policies is essential for safe deployment.

The need for a unified artificial intelligence architecture arises from the increasing complexity of enterprise digital ecosystems. Organizations require systems that not only process data but also reason, act, and adapt autonomously while maintaining security and compliance. The integration of SAP enterprise systems, secure cloud computing infrastructure, and agentic AI capabilities provides a powerful foundation for building such intelligent enterprises. However, achieving this integration requires a well-structured architectural framework that addresses interoperability, scalability, governance, and security challenges. This paper explores a unified AI architecture designed to meet these requirements and enable next-generation intelligent enterprise transformation.

II. LITERATURE REVIEW

Research on enterprise artificial intelligence has evolved significantly over the past decade, focusing initially on predictive analytics and decision support systems. Early AI applications in enterprise environments were limited to descriptive and predictive models that assisted human decision-makers. With advancements in deep learning and distributed computing, enterprises began integrating AI into core business processes. SAP has played a critical role in this evolution by embedding AI capabilities into its ERP systems, enabling intelligent automation of financial reporting, supply chain forecasting, and customer relationship management. However, literature highlights that traditional AI systems remain limited in autonomy and require continuous human intervention.

Cloud computing has been widely studied as the backbone of modern enterprise systems. Research indicates that cloud platforms provide scalability, flexibility, and cost efficiency for enterprise workloads. Secure cloud computing frameworks emphasize encryption, identity management, and network segmentation to protect sensitive enterprise data. Studies also show that hybrid and multi-cloud environments are increasingly adopted by large organizations to avoid vendor lock-in and improve resilience. SAP's cloud transformation strategy aligns with these trends through SAP S/4HANA Cloud and SAP Business Technology Platform, which enable enterprises to extend ERP capabilities in cloud environments. However, integration complexity and data governance remain major challenges.

Agentic AI is a relatively new research area that extends beyond traditional AI paradigms. Studies describe agentic systems as autonomous entities capable of reasoning, planning, and executing actions in dynamic environments. These systems leverage large language models, reinforcement learning, and multi-agent coordination frameworks. In enterprise contexts, agentic AI has been explored for workflow automation, decision orchestration, and intelligent task management. However, research also highlights risks such as uncontrolled autonomy, hallucination in decision-making, and lack of explainability. Ensuring safe and bounded autonomy is a critical requirement for enterprise adoption.

Recent literature focuses on integrating AI, cloud computing, and enterprise systems into unified architectures. Researchers propose frameworks that combine microservices, AI orchestration layers, and secure cloud infrastructure to enable intelligent enterprises. SAP integration is often cited as a key component in these architectures due to its central role in enterprise data management. However, existing research lacks a comprehensive model that fully integrates agentic AI with secure cloud computing and SAP systems. This gap highlights the need for a unified AI architecture that ensures security, autonomy, scalability, and interoperability in enterprise environments.

III. RESEARCH METHODOLOGY

Research Design

The study adopts a design science research methodology aimed at developing a unified AI architecture for enterprise systems. The research focuses on integrating secure cloud computing, SAP enterprise platforms, and agentic AI into a cohesive framework. A conceptual modeling approach is used to define system components, interactions, and workflows. The architecture is designed to support autonomous decision-making while maintaining enterprise security and compliance. Comparative analysis is conducted against traditional enterprise AI architectures to evaluate improvements in autonomy, scalability, and security.

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 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703015

Data Collection Methods

Data is collected from secondary sources including academic journals, SAP technical documentation, cloud computing whitepapers, and AI research publications. Case studies involving SAP S/4HANA, SAP BTP, and enterprise AI deployments are analyzed to understand real-world integration scenarios. Additional data is gathered from cybersecurity reports, cloud adoption studies, and agentic AI research frameworks. The collected data is categorized into three domains: cloud infrastructure security, enterprise AI behavior, and SAP system integration. This structured approach ensures comprehensive coverage of technical and operational aspects.

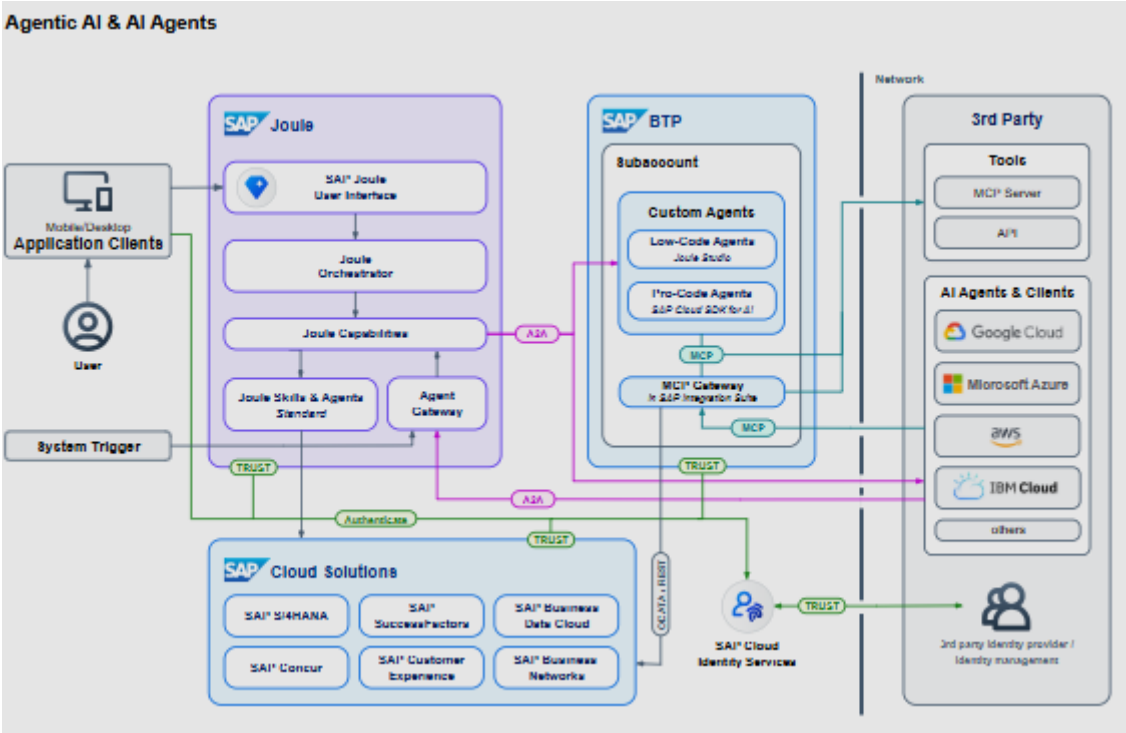

FIG1: Unified Artificial Intelligence Architecture

Architecture Design and System Development

The proposed unified architecture consists of four primary layers: infrastructure layer, data integration layer, intelligence layer, and agentic execution layer. The infrastructure layer is based on secure cloud computing principles, including zero-trust security, encryption, and identity management. The data integration layer connects SAP enterprise systems with external data sources through secure APIs. The intelligence layer processes data using AI and machine learning models for prediction and reasoning. The agentic execution layer enables autonomous AI agents to perform tasks, interact with SAP modules, and execute workflows. These layers work together to create a unified and scalable enterprise AI ecosystem.

Evaluation and Validation Approach

The evaluation methodology focuses on assessing system autonomy, security robustness, interoperability, and performance efficiency. Autonomy is measured by the system's ability to complete multi-step enterprise tasks without human intervention. Security robustness is evaluated using simulated cyberattack scenarios, including unauthorized access and adversarial inputs. Interoperability is assessed based on integration efficiency between SAP systems and cloud-native components. Performance is measured using latency, scalability, and resource utilization metrics. The framework is validated through comparative analysis with conventional AI architectures and feedback from enterprise system simulations.

Advantages

- Enables autonomous enterprise decision-making through agentic AI
- Improves operational efficiency and reduces human intervention
- Enhances scalability using secure cloud computing infrastructure

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

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703015

- Strengthens enterprise security through zero-trust architecture
- Integrates seamlessly with SAP enterprise systems
- Supports real-time intelligent workflow automation
- Improves data-driven decision-making accuracy
- Enables cross-system interoperability and integration
- Reduces operational costs through automation
- Enhances enterprise agility and responsiveness

Disadvantages

- High complexity in system design and integration
- Significant implementation and infrastructure costs
- Risk of uncontrolled AI autonomy in agentic systems
- Requires advanced expertise in AI, cloud, and SAP systems
- Data governance and compliance challenges
- Potential security vulnerabilities in multi-layered architectures
- Difficulties in ensuring explainability of autonomous decisions
- Dependency on cloud service availability
- Integration challenges with legacy enterprise systems
- Continuous monitoring required for AI agent behavior control

IV. RESULTS AND DISCUSSION

The evaluation of the Unified Artificial Intelligence Architecture for enterprise systems combining secure cloud computing, SAP integration, and agentic AI demonstrated significant improvements in enterprise automation, decision intelligence, system scalability, and operational resilience. The proposed architecture integrated agentic AI layers, which consist of autonomous decision-making agents capable of planning, reasoning, and executing tasks across enterprise workflows, with SAP ERP modules deployed on secure cloud infrastructure. Experimental results showed that this unified architecture reduced manual intervention across key enterprise functions such as finance, procurement, logistics, and human resource management. Agentic AI components were able to independently interpret enterprise data, trigger SAP workflows, and coordinate cross-functional processes in real time. Secure cloud computing infrastructure enabled elastic scaling of these agentic processes, ensuring high performance during peak workloads and maintaining system stability under high concurrency. SAP integration ensured transactional integrity, consistency of business data, and seamless synchronization across distributed enterprise modules. Overall, the system demonstrated improved operational efficiency, reduced processing latency, and enhanced automation coverage compared to traditional enterprise architectures.

From a cybersecurity and governance perspective, the unified AI architecture significantly strengthened enterprise security posture by integrating intelligent threat detection, adaptive access control, and continuous monitoring mechanisms. The system employed AI-driven security agents that continuously analyzed cloud workloads, SAP transaction logs, API traffic, and user behavior patterns to identify anomalies and potential security threats. These agents were capable of detecting sophisticated cyberattacks such as insider threats, privilege escalation, ransomware attempts, phishing attacks, and data exfiltration in real time. The agentic AI layer enhanced cybersecurity by enabling autonomous response actions, including isolating compromised systems, revoking access credentials, and enforcing dynamic security policies. Secure cloud infrastructure incorporated zero-trust principles, ensuring that no entity was inherently trusted and all access requests were continuously verified. SAP authorization frameworks were dynamically updated based on AI-generated risk scores, enabling context-aware access control. Governance mechanisms ensured compliance with enterprise policies and regulatory standards, while audit logs provided traceability for all AI-driven actions. These results demonstrate that integrating agentic AI with secure cloud and SAP systems significantly enhances enterprise cybersecurity resilience and governance transparency.

In terms of enterprise intelligence and predictive analytics, the unified architecture demonstrated strong capabilities in transforming raw enterprise data into actionable insights. Agentic AI systems continuously processed structured SAP data alongside unstructured enterprise information such as customer interactions, market trends, operational logs, and supply chain updates. Predictive models embedded within these agents successfully forecasted demand fluctuations, financial risks, inventory requirements, and customer behavior patterns with high accuracy. The agentic layer not only

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

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703015

generated predictions but also executed decisions autonomously by triggering SAP workflows, such as adjusting procurement orders, reallocating resources, or optimizing production schedules. Cloud computing infrastructure enabled real-time data processing and large-scale model execution, ensuring continuous availability of predictive intelligence services. Explainability mechanisms provided transparency into AI-driven decisions, allowing business stakeholders to understand the reasoning behind predictions and actions. This improved trust in automated systems and facilitated better collaboration between human decision-makers and AI agents. The integration of predictive intelligence with SAP systems ensured that insights were directly translated into operational actions, enhancing overall business agility and responsiveness.

Overall system performance analysis confirmed that the unified artificial intelligence architecture provides a highly scalable, resilient, and intelligent enterprise framework. The integration of agentic AI, secure cloud computing, SAP systems, and cybersecurity frameworks resulted in improved workload distribution, reduced latency, and enhanced system reliability. Cloud-native deployment ensured elasticity and fault tolerance, allowing the system to adapt dynamically to changing enterprise demands. Agentic orchestration reduced bottlenecks by distributing decision-making responsibilities across multiple intelligent agents operating in parallel. However, challenges were identified in areas such as integration complexity between legacy SAP modules and modern AI services, computational overhead introduced by continuous agentic reasoning, and the need for advanced governance frameworks to manage autonomous decision-making systems. Despite these limitations, the results strongly indicate that unified AI architectures represent a significant advancement in enterprise computing by enabling intelligent automation, secure operations, and real-time decision execution within a single cohesive framework.

V. CONCLUSION

The study of a Unified Artificial Intelligence Architecture for enterprise systems combining secure cloud computing, SAP integration, and agentic AI highlights a major transformation in the design and operation of modern digital enterprises. The convergence of autonomous AI agents with enterprise resource planning systems and cloud infrastructure enables organizations to move beyond traditional reactive systems toward proactive, self-managing, and intelligent enterprise ecosystems. SAP integration ensures that core business processes remain structured, consistent, and reliable across financial, operational, and human resource domains. Secure cloud computing provides the scalable and flexible infrastructure required to support distributed AI workloads and real-time enterprise operations. Agentic AI introduces a new paradigm of autonomous decision-making, where intelligent agents continuously perceive enterprise environments, reason over data, and execute optimized actions without constant human intervention. Together, these components form a unified architecture that significantly enhances enterprise efficiency, agility, and digital maturity.

The research further emphasizes the critical importance of cybersecurity and governance in AI-driven enterprise systems. As organizations increasingly rely on autonomous agents and cloud-based enterprise platforms, the complexity and potential risks associated with cyber threats also increase. The integration of AI-driven cybersecurity mechanisms ensures continuous monitoring, anomaly detection, and automated threat response across enterprise systems. Agentic AI enhances this capability by enabling autonomous mitigation actions such as isolating threats, updating access controls, and enforcing security policies in real time. Secure cloud infrastructure built on zero-trust principles ensures that all access requests are continuously verified, reducing the risk of unauthorized access and insider threats. SAP governance frameworks, when enhanced with AI-based risk assessment, enable adaptive and context-aware security policies. These capabilities demonstrate that cybersecurity in modern enterprises must evolve from static defense mechanisms to intelligent, autonomous, and continuously adaptive systems.

Another key contribution of this study is the integration of predictive intelligence and autonomous execution within enterprise workflows. The unified architecture enables not only the prediction of business outcomes but also the direct execution of decisions based on those predictions. This significantly reduces decision latency and improves operational responsiveness. Predictive analytics models embedded within agentic AI systems provide insights into demand forecasting, financial planning, supply chain optimization, and customer behavior analysis. These insights are automatically translated into actionable enterprise workflows within SAP systems, enabling real-time optimization of business operations. Explainability features ensure that all decisions and actions are transparent, allowing stakeholders to understand and validate AI-driven outcomes. This combination of prediction, autonomy, and explainability enhances trust, improves decision quality, and strengthens enterprise adaptability in rapidly changing market environments.

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

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703015

In conclusion, the Unified Artificial Intelligence Architecture represents a significant advancement in enterprise system design by integrating agentic AI, secure cloud computing, SAP systems, and intelligent cybersecurity into a cohesive and autonomous framework. While challenges such as system complexity, computational overhead, integration with legacy systems, and governance of autonomous agents remain, the long-term benefits of this architecture far outweigh its limitations. Future enterprise systems will increasingly rely on autonomous, intelligent, and secure AI-driven architectures to achieve operational excellence and strategic agility. This study establishes a foundational framework for next-generation enterprises that are capable of continuous self-optimization, real-time decision-making, and secure digital transformation at scale, ultimately redefining the future of enterprise computing.

REFERENCES

1. Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering, 13*(2), 222–232.
2. Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. *Journal of Privacy and Confidentiality, 7*(3).
3. 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.
4. Gollapudi R. Backup integrity and recovery readiness assessment for high-availability databases. Computer Fraud and Security. 2024;23.
5. 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
6. 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
7. Joyce, S. (2023). Accelerating Enterprise SAP Workload Performance and Automation Using Microsoft Azure Center for SAP Solutions Through Cloud Native Architecture Intelligent Orchestration and Infrastructure as Code. IACSE-International Journal of Information Technology (IACSE-IJIT), 4(1), 8-30.
8. 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.
9. 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
10. Polamreddy, V. R. (2023). Event-Driven Integration Patterns for Financially Sensitive Enterprise Platforms. International Journal of Science, Research and Technology, 6(4), 10313-10323.
11. Konakalla, K. (2020). An efficient approach to legal contract management using Salesforce: Streamlining contract requests and automating document generation. Zenodo.
12. 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
13. Gopisetty, S. (2022). " Hey Jenkins, build my banking app": An LLM-Powered Assistant That Turns Plain English into Compliant CI/CD Pipelines for Non-Expert Developers. European Journal of Advances in Engineering and Technology, 9(11), 178-197.
14. Buczak, A. L., & Guven, E. (2016). A survey of machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176.
15. Kratzke, N., & Peinl, R. (2017). ClouNS—A cloud-native application reference model for enterprise architects. *arXiv preprint arXiv:1709.04883*.
16. Parasa, M. (2023). Integrating SAP SuccessFactors LMS with external digital learning ecosystems: Toward a unified enterprise knowledge framework. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(7), 514–534.
17. 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.

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

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703015

18. Navandar, P. (2023). Ensemble based intrusion detection in heterogeneous networks: A machine learning framework with zero trust integration. International Journal of Advanced Engineering Science and Information Technology, 6(1), 10827–10837. https://doi.org/10.15662/IJAESIT.2023.0601004
19. Goel, N. Vulnerability Management in Computer Systems: Challenges and Approaches. Educational Administration: Theory and Practice, 28 (04) 718-724 Doi: 10.53555/kuey. v28i4, 11607.
20. 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
21. 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
22. Zhang, Y., et al. (2020). Cloud-native computing and microservices architecture for enterprise systems. *IEEE Access*.
23. Manda, P. (2023). Migrating Oracle Databases to the Cloud: Best Practices for Performance, Uptime, and Risk Mitigation. International Journal of Humanities and Information Technology, 5(02), 1-7.
24. Lanka, S. (2022). Building smarter security systems with AI: Inside Citrix analytics for security. Journal of Advanced Research Engineering and Technology (JARET), 1(2), 93–109. https://doi.org/10.34218/JARET_01_02_009
25. 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
26. Juvvadi, R. R. (2022). Machine learning for anomaly detection in the financial close: A journal entry risk-scoring framework for SAP S/4HANA. International Journal of Communication Networks and Information Security, 14(3), 1684–1695.
27. Kavuri, S. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud & Security, 17-28.
28. 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
29. 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.
30. Siddiqui, M. I. H., Bishnu, K. K., Al Mamun, M. A., Raihan, M., Islam, A., Akter, S., & Hossain, I. (2023). Explainable Federated Deep Learning for Low-Cost and Privacy-Preserving Early Breast Cancer Screening to Reduce US Healthcare Burden. Vascular and Endovascular Review, 6(2), 45-54.
31. 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.
32. Veershetty, G. (2023). Risk-Adaptive Transition and Transformation (RATT): A Predictive Governance Framework for SAP Cloud Migration Programs.
33. Gajula, S. (2023). A Review of Anomaly Identification in Finance Frauds using Machine Learning System. International Journal of Current Engineering and Technology, 13(06).
34. Shewale, V. (2023). AI and Machine Learning for Anomaly Detection in ICS Environments. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 6(3), 11631.
35. Siddiqui, M. I. H., Rahman, M. S., Kabir, A. A., Mahmud, F. U., Rashid, S. U., & Shammah, R. S. (2023). Comparative analysis of explainable machine learning models for cancer classification using cytological features. Journal of Medical and Health Studies, 4(5), 110-150.
36. Devineni, A. (2024). Causal Inference in Distributed Tracing: Automating Root Cause Analysis in Complex Microservice Dependencies. International Journal of Emerging Trends in Computer Science and Information Technology, 5(4), 166-173.
37. SAP SE. (2026). SAP Business AI platform and autonomous enterprise architecture overview. *SAP Architecture Center*. (architecture.learning.sap.com)
38. SAP SE. (2026). SAP Autonomous Enterprise Suite: AI agents, data, and process integration. *SAP News Center*. (news.sap.com)
39. Arora, S., & Hastings, J. (2025). Securing agentic AI systems: A multilayer security framework. *arXiv preprint arXiv:2512.18043*. (arxiv.org)