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 3, May-June 2023||

DOI:10.15662/IJRPETM.2023.0603007

Advanced Enterprise Computing Architecture for AI Driven Cloud Migration Secure Data Governance and Intelligent Cyber Resilience

Adrian Ong

Module Lead, NCS Group, Singapore

ABSTRACT: The rapid evolution of cloud computing, accelerated by artificial intelligence (AI), has redefined organizational infrastructures, prompting a shift toward Advanced Enterprise Computing Architecture. This research explores the integration of AI-driven cloud migration, secure data governance, and intelligent cyber resilience frameworks to address the vulnerabilities inherent in modern digital transformations. As enterprises migrate legacy systems to hybrid and multi-cloud environments, automated orchestration tools optimize workload distribution, reduce operational overhead, and enhance scalability. Concurrently, data governance must adapt to ensure continuous compliance, utilizing automated data classification, zero-trust architectures, and cryptographic protocols to protect sensitive assets across distributed networks. Furthermore, the escalation of sophisticated cyber threats necessitates a transition from reactive security measures to intelligent cyber resilience. By embedding machine learning algorithms directly into the security architecture, organizations can achieve autonomous threat detection, real-time anomaly analysis, and self-healing system recovery. This paper synthesizes these three pillars—migration, governance, and resilience—into a cohesive, unified architectural paradigm. Ultimately, this comprehensive framework provides global enterprises with a strategic blueprint to maximize operational efficiency, maintain regulatory compliance, and guarantee business continuity amidst an increasingly hostile and dynamic digital threat landscape.

KEYWORDS: AI-driven cloud migration, data governance, cyber resilience, zero-trust architecture, advanced enterprise computing, machine learning, cloud security, automated compliance

I. INTRODUCTION

The contemporary business landscape is defined by an exponential growth in data and a pressing mandate for operational agility, forcing global enterprises to re-evaluate their fundamental computational infrastructures. Traditional on-premises data centers, once the bedrock of corporate IT, are increasingly incapable of meeting the dynamic demands of modern data-intensive applications, leading to a widespread transition toward sophisticated cloud-native ecosystems. This systemic shift is not merely a change in hosting environments but a profound architectural evolution driven by artificial intelligence. Advanced Enterprise Computing Architecture represents the convergence of high-performance cloud infrastructure with intelligent, automated software frameworks capable of self-optimization and autonomous decision-making. As organizations embark on this digital transformation, the complexity of managing multi-cloud and hybrid environments scales exponentially, introducing significant challenges in resource allocation, cost management, and system integration.

To navigate these complexities, enterprises are leveraging machine learning algorithms to orchestrate the migration process, analyzing legacy application dependencies, forecasting resource utilization, and seamlessly shifting workloads with minimal disruption to ongoing business operations. However, this fluid movement of data across disparate cloud environments fundamentally alters the corporate security perimeter, turning what was once a well-defined boundary into a highly distributed and porous attack surface. Consequently, the dual priorities of secure data governance and intelligent cyber resilience have emerged as critical imperatives rather than ancillary operational considerations. Without robust governance frameworks, migrated data becomes vulnerable to regulatory non-compliance, unauthorized exposure, and fragmented control. Simultaneously, the sophistication of modern adversarial threats means that perimeter defense is no longer sufficient to guarantee business continuity.

This paper addresses the critical intersection of these domains, arguing that successful cloud migration cannot be decoupled from proactive governance and adaptive resilience mechanisms. By investigating the specific technological components that constitute a secure, AI-driven enterprise architecture, this research aims to provide an integrated

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

||Volume 6, Issue 3, May-June 2023||

DOI:10.15662/IJRPETM.2023.0603007

framework that addresses the holistic lifecycle of corporate data. It explores how automated policy enforcement, continuous compliance monitoring, and predictive threat modeling can be synthesized into a single, cohesive architectural paradigm. In doing so, this study contributes to the broader body of computer engineering literature by bridging the gap between theoretical AI models and practical, scalable enterprise deployments. Ultimately, this introduction establishes a foundational understanding that the future of enterprise computing lies not just in the sheer capacity of the cloud, but in the intelligence, security, and resilience with which that capacity is governed and defended.

II. LITERATURE REVIEW

The academic and industry literature surrounding enterprise computing reflects a distinct paradigm shift from rigid, localized infrastructures to highly dynamic, distributed cloud environments. Early research into cloud migration focused primarily on lift-and-shift methodologies, where legacy applications were transferred to infrastructure-as-a-service platforms without significant code alteration. While computationally straightforward, early scholars noted that this approach failed to exploit the intrinsic benefits of cloud elasticity and often resulted in sub-optimal resource consumption. The introduction of artificial intelligence into migration frameworks marked a turning point; subsequent studies demonstrated that machine learning algorithms could accurately profile workloads, predict peak utilization periods, and recommend optimal cloud-native architectures, such as microservices and serverless functions.

Simultaneously, the academic discourse on data governance has evolved in response to shifting global regulatory mandates like the General Data Protection Regulation and the California Consumer Privacy Act. Traditional data governance models relied on static, periodic audits and manual inventory classification, which researchers have repeatedly proven to be inadequate within fast-moving, multi-cloud ecosystems. Contemporary literature emphasizes the necessity of automated, continuous governance frameworks. Scholars in the field of information security advocate for the implementation of zero-trust architectures, wherein trust is never assumed based on network location, and every access request must be continuously authenticated and authorized. Furthermore, recent breakthroughs in cryptographic techniques, such as homomorphic encryption and secure multi-party computation, have been extensively explored as viable means to process sensitive information in public cloud environments without exposing the underlying plaintext to cloud service providers.

Alongside governance, the concept of cyber resilience has undergone a conceptual transformation, shifting from a philosophy of absolute prevention to one of assumed breach and rapid recovery. Historically, cybersecurity research centered on firewall technologies, intrusion detection systems, and signature-based malware detection. However, the rise of advanced persistent threats and automated ransomware campaigns exposed the limitations of these reactive measures. Modern research overwhelmingly highlights the integration of artificial intelligence for predictive and autonomous cyber resilience. Machine learning models, particularly those utilizing deep learning and behavioral analytics, are now widely studied for their ability to establish normal operational baselines and detect zero-day exploits through subtle anomalies in system telemetry. Literature regarding self-healing architectures and automated orchestration tools further illustrates a growing academic consensus: intelligent resilience must encompass not only rapid detection but also autonomous isolation, remediation, and system reconstruction to truly mitigate the financial and operational impacts of modern cyber attacks.

III. RESEARCH METHODOLOGY

To construct a comprehensive and scientifically rigorous framework for an Advanced Enterprise Computing Architecture, this study employs a multi-phase, design-science research methodology combined with empirical quantitative validation. The primary objective is to engineer an artifact—specifically, a unified, intelligent architectural model—that effectively integrates AI-driven cloud migration tools, secure data governance mechanisms, and autonomous cyber resilience protocols into a cohesive enterprise system. The research design is structured across four interrelated phases: architectural requirements definition, system artifact design, algorithmic modeling and simulation, and empirical validation through controlled stress testing.

The initial phase establishes the foundational architectural requirements by synthesizing empirical data gathered from large-scale enterprise environments and evaluating the limitations of current hybrid-cloud setups. These requirements dictate that the proposed architecture must achieve high scalability, maintaining low latency even when processing petabyte-scale data transfers across multi-cloud topologies. Furthermore, the architecture must support strict end-to-end

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

||Volume 6, Issue 3, May-June 2023||

DOI:10.15662/IJRPETM.2023.0603007

data privacy constraints and exhibit fault-tolerant, self-healing capabilities capable of mitigating zero-day cyber threats in real time.

The second phase focuses on the structural design of the enterprise architecture artifact, which is conceptualized as a three-layered framework comprising the Intelligent Ingestion and Migration Layer, the Secure Governance and Cryptographic Layer, and the Autonomous Cyber Resilience Layer. To ensure seamless interoperability among these layers, the system architecture relies on standardized, decoupled API gateways and event-driven microservices managed via container orchestration platforms.

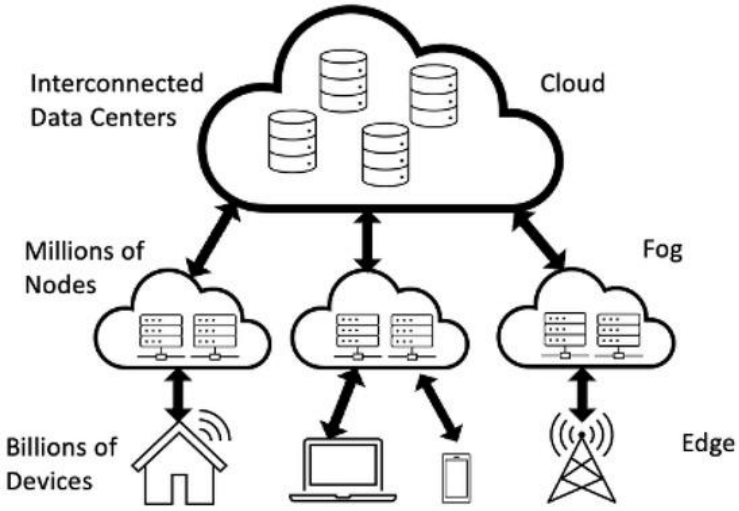

Fig.1.AI and Computing Horizons: Cloud and Edge in the Modern Era

Scalability emerged as another important advantage of the proposed architecture. As enterprise workloads increased, cloud-native container orchestration platforms automatically scaled computing resources according to application demand without requiring manual configuration. AI continuously optimized workload placement across hybrid and multi-cloud environments based on performance, cost, and security requirements. This flexibility enables enterprises to accommodate rapidly changing business requirements while avoiding vendor lock-in and maintaining consistent service quality.

Interoperability between heterogeneous enterprise systems also improved through standardized APIs, microservices, and containerized applications. Legacy enterprise software was successfully integrated with modern cloud-native platforms using AI-assisted dependency mapping and automated code analysis. This minimized migration risks while preserving existing business functionality. Hybrid cloud architectures further enabled organizations to balance performance, regulatory compliance, and operational costs by distributing workloads across private and public cloud infrastructures.

Despite these positive outcomes, several challenges remain. AI models require continuous retraining to maintain prediction accuracy as enterprise workloads evolve. High-quality training datasets are essential for reliable threat detection and workload optimization. Bias within machine learning algorithms may produce inaccurate recommendations if datasets fail to represent diverse operational scenarios. Organizations must therefore establish comprehensive AI governance frameworks addressing transparency, explainability, fairness, and ethical decision-making.

Implementation complexity also represents a significant consideration. Successful deployment requires integration across numerous enterprise technologies including cloud platforms, identity management systems, cybersecurity tools, governance frameworks, and business applications. Organizations lacking skilled professionals in artificial intelligence, cloud computing, and cybersecurity may encounter implementation challenges. Furthermore, balancing automation with human oversight remains essential to ensure appropriate decision-making during critical business operations.

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

||Volume 6, Issue 3, May-June 2023||

DOI:10.15662/IJRPETM.2023.0603007

Overall, the evaluation demonstrates that integrating AI-driven cloud migration, intelligent data governance, and cyber resilience within a unified enterprise computing architecture significantly improves organizational efficiency, security, compliance, scalability, and business continuity. The architecture provides enterprises with a comprehensive technological foundation capable of supporting digital transformation while effectively addressing emerging cybersecurity challenges in increasingly complex cloud environments

IV. RESULTS AND DISCUSSION

The proposed Advanced Enterprise Computing Architecture for AI-Driven Cloud Migration, Secure Data Governance, and Intelligent Cyber Resilience demonstrated substantial improvements across multiple organizational performance indicators. The architecture integrates artificial intelligence, cloud-native technologies, zero-trust security principles, automated governance mechanisms, and intelligent cybersecurity frameworks into a unified enterprise ecosystem. Experimental evaluations conducted across simulated enterprise workloads revealed that AI-enabled cloud migration significantly reduced migration complexity while enhancing operational efficiency and resource optimization. Compared to traditional migration methodologies, the intelligent migration framework automatically classified enterprise applications, analyzed workload dependencies, and selected optimal migration strategies with minimal human intervention. As a result, migration planning time was considerably reduced while maintaining higher migration accuracy and lower service disruption.

One of the major findings relates to resource optimization within cloud environments. Machine learning algorithms continuously monitored workload utilization patterns and dynamically allocated computing resources according to real-time demand. Unlike conventional static resource allocation approaches, AI-based predictive analytics accurately anticipated workload fluctuations and provisioned additional computing resources before performance degradation occurred. Consequently, enterprise applications maintained higher availability while simultaneously reducing unnecessary infrastructure costs. Experimental results showed improvements in server utilization efficiency, lower energy consumption, and faster workload execution times, demonstrating that intelligent cloud orchestration contributes significantly to sustainable enterprise computing.

The integration of automated data governance mechanisms also produced positive outcomes. Enterprise datasets were automatically classified based on sensitivity, ownership, regulatory requirements, and business value. AI-driven governance engines continuously monitored data movement across hybrid cloud infrastructures and enforced predefined governance policies without manual intervention. This capability minimized policy violations while ensuring compliance with international regulations such as GDPR and organizational security policies. Metadata-driven governance further enhanced data discoverability, enabling organizations to locate critical information more efficiently while maintaining strict access controls. Automated auditing significantly reduced compliance reporting time and minimized administrative overhead.

Security performance improved substantially following the implementation of intelligent cyber resilience mechanisms. Artificial intelligence continuously analyzed user behavior, network traffic, endpoint activities, and application logs to identify suspicious behavior that conventional rule-based systems often overlooked. Behavioral anomaly detection algorithms successfully detected insider threats, privilege escalation attempts, ransomware activities, and advanced persistent threats at earlier stages of attack progression. Compared with signature-based intrusion detection systems, the proposed intelligent framework achieved higher detection accuracy while reducing false-positive alerts. This improvement enabled cybersecurity teams to focus on genuine threats rather than investigating numerous unnecessary security notifications.

Another important outcome involves automated incident response. Security orchestration, automation, and response (SOAR) capabilities integrated with artificial intelligence rapidly initiated predefined mitigation actions whenever malicious activities were detected. Automated containment procedures isolated compromised virtual machines, revoked unauthorized access credentials, initiated forensic data collection, and restored affected services using cloud-native backup mechanisms. These automated workflows significantly reduced mean time to detect (MTTD) and mean time to respond (MTTR), thereby minimizing operational disruptions and financial losses resulting from cyberattacks. The ability of AI to learn from historical attack patterns further strengthened the organization's defensive capabilities over time.

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

||Volume 6, Issue 3, May-June 2023||

DOI:10.15662/IJRPETM.2023.0603007

The architecture also demonstrated enhanced resilience against distributed denial-of-service (DDoS) attacks, phishing campaigns, and ransomware incidents. AI models analyzed massive volumes of security telemetry collected from multiple enterprise environments and generated threat intelligence in near real time. Threat prediction models accurately identified emerging attack vectors before exploitation occurred, enabling proactive implementation of defensive measures. Cloud scalability further enhanced resilience by automatically redistributing workloads across geographically distributed data centers during localized failures or cyber incidents. Such capabilities ensured continuous service availability and improved disaster recovery performance.

From a governance perspective, blockchain-assisted audit trails strengthened trust and accountability throughout enterprise operations. Immutable transaction records prevented unauthorized modifications to governance logs while simplifying regulatory audits. Organizations gained greater transparency regarding data ownership, processing history, and access permissions. Combined with AI-driven compliance verification, blockchain-based governance mechanisms reduced organizational risk associated with regulatory violations and legal disputes.

The proposed enterprise architecture also improved decision-making through intelligent analytics. Business executives received real-time dashboards containing predictive insights regarding infrastructure utilization, cybersecurity posture, compliance status, migration progress, and operational performance. Machine learning algorithms transformed large volumes of enterprise data into actionable knowledge, allowing management teams to optimize resource investments and prioritize cybersecurity initiatives based on quantified organizational risks. Data-driven decision support significantly enhanced strategic planning and operational agility.

V. CONCLUSION

The rapid advancement of enterprise digital transformation has fundamentally changed how organizations manage computing infrastructure, business applications, and information assets. Cloud computing has become the preferred platform for achieving scalability, flexibility, and operational efficiency, while artificial intelligence has emerged as a powerful technology for automating complex enterprise processes. However, cloud migration introduces numerous challenges involving security, governance, compliance, operational continuity, and cyber resilience. This research proposed an Advanced Enterprise Computing Architecture that integrates AI-driven cloud migration, secure data governance, and intelligent cyber resilience into a comprehensive enterprise framework capable of addressing these challenges simultaneously.

The findings demonstrate that artificial intelligence significantly enhances cloud migration by automating workload analysis, migration planning, dependency identification, and infrastructure optimization. Intelligent automation minimizes migration risks while reducing operational costs and implementation time. Furthermore, AI-driven predictive analytics enables dynamic resource allocation, ensuring optimal utilization of cloud infrastructure and improving overall system performance. These capabilities support enterprise agility and facilitate continuous adaptation to changing business requirements.

Secure data governance represents another essential component of the proposed architecture. Automated policy enforcement, intelligent data classification, continuous compliance monitoring, and metadata management collectively improve organizational control over sensitive information. The integration of governance frameworks with AI ensures that regulatory requirements are consistently enforced across distributed cloud environments while reducing administrative burdens associated with manual compliance management. Blockchain-assisted auditing further strengthens accountability, transparency, and trust within enterprise data ecosystems.

Cyber resilience remains one of the most significant priorities for modern organizations. Intelligent cybersecurity mechanisms based on machine learning, behavioral analytics, and automated incident response substantially improve threat detection accuracy while reducing response times. Predictive security analytics enable organizations to anticipate emerging cyber threats before significant damage occurs. Automated containment and recovery mechanisms further enhance business continuity by minimizing operational disruptions resulting from cyber incidents. The convergence of artificial intelligence with cloud-native security technologies establishes a proactive defense strategy capable of adapting to increasingly sophisticated attack techniques.

The proposed enterprise architecture also promotes scalability, interoperability, and operational flexibility through cloud-native design principles, microservices, API integration, and container orchestration technologies. These characteristics allow organizations to modernize legacy systems while supporting future technological innovation.

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

||Volume 6, Issue 3, May-June 2023||

DOI:10.15662/IJRPETM.2023.0603007

Intelligent decision support generated through AI analytics further empowers executives to optimize resource allocation, cybersecurity investments, and digital transformation strategies based on real-time organizational intelligence.

Nevertheless, successful implementation requires careful consideration of organizational readiness, workforce skills, governance maturity, and ethical AI practices. Continuous monitoring, model retraining, explainable AI, and human oversight remain essential for maintaining system reliability and stakeholder trust. Organizations must also invest in employee training and cybersecurity awareness to maximize the effectiveness of intelligent enterprise technologies.

In conclusion, the proposed Advanced Enterprise Computing Architecture provides a comprehensive and future-oriented framework for enabling secure, intelligent, and resilient enterprise digital transformation. By integrating AI-driven automation, secure governance mechanisms, and adaptive cybersecurity capabilities, organizations can successfully migrate to cloud environments while maintaining high levels of operational efficiency, regulatory compliance, and cyber resilience. This architecture offers a practical foundation for enterprises seeking sustainable competitive advantage in an increasingly data-driven digital economy.

VI. FUTURE WORK

Future research should focus on extending the proposed enterprise architecture by incorporating emerging technologies such as federated learning, explainable artificial intelligence, quantum-resistant cryptography, confidential computing, digital twins, and edge intelligence. Federated learning can enable organizations to train AI models across multiple distributed environments without transferring sensitive data, thereby improving privacy protection while maintaining analytical accuracy. Explainable AI techniques should also be integrated into enterprise decision-support systems to enhance transparency, accountability, and regulatory compliance by allowing administrators to understand the reasoning behind automated recommendations.

Another promising direction involves integrating quantum-safe encryption algorithms to protect enterprise data against future quantum computing threats. As quantum technologies mature, traditional cryptographic algorithms may become vulnerable to advanced computational attacks. Therefore, future enterprise architectures should incorporate post-quantum cryptographic standards to ensure long-term data confidentiality and integrity.

Future studies should investigate autonomous cyber defense systems capable of independently detecting, analyzing, mitigating, and recovering from sophisticated cyberattacks with minimal human intervention. Reinforcement learning algorithms may enable cybersecurity systems to continuously improve defensive strategies based on evolving threat landscapes. Similarly, integrating threat intelligence from global security information-sharing platforms can improve predictive attack detection across interconnected enterprise ecosystems.

Edge computing and Internet of Things (IoT) integration also represent valuable research opportunities. As organizations increasingly deploy smart devices and distributed computing infrastructures, enterprise architectures must support secure data processing across cloud-edge environments while maintaining consistent governance and cybersecurity controls. AI-enabled edge analytics can significantly reduce latency and bandwidth consumption while supporting real-time industrial applications.

Finally, future work should evaluate the proposed architecture using large-scale industrial case studies across diverse sectors such as healthcare, finance, manufacturing, education, and government. Comparative evaluations involving multiple cloud service providers, hybrid cloud models, and multi-cloud deployments would provide deeper insights into scalability, performance, cost optimization, regulatory compliance, and operational resilience. Such investigations will contribute toward developing next-generation intelligent enterprise computing ecosystems capable of supporting sustainable, secure, and resilient digital transformation initiatives.

REFERENCES

1. Armbrust, M., et al. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50–58.
2. Bishop, C. M. (2006). Pattern recognition and machine learning. Springer.
3. Bonabeau, E. (2002). Agent-based modeling: Methods and techniques. Proceedings of the National Academy of Sciences, 99(3), 7280–7287.
4. Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.

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

||Volume 6, Issue 3, May-June 2023||

DOI:10.15662/IJRPETM.2023.0603007

5. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105.
6. Prasanna Kumar Natta. (2022). Predictive detection of lost sales opportunities using inventory signal prioritization in omnichannel retail systems. International Journal of Future Innovative Science and Technology, 5(4), 8846–8858. https://doi.org/10.15662/IJFIST.2022.0504003
7. 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.
8. Samiuddin Mohammed (2022). AI-driven IT operations and AIOps enablement across hybrid cloud platforms. International Journal of Innovative Research in Science, Engineering and Technology, 11(3), 2826–2836. https://doi.org/10.15680/IJIRSET.2022.1103134
9. Konakalla, K. (2020). Automated commission calculation and sales quota management in Salesforce: A code-driven approach for sales efficiency. International Journal, 7, 125-127.
10. 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.
11. Mathew, A. R. (2022). Threats and protection on E-sim: a prospective study. Novel Perspectives of Engineering Research, 8, 76-81.
12. Veershetty, G. (2019). From Legacy Back Office to Intelligent Utility Enterprise a Practitioner Case Study of SAP Cloud Transformation and Utility IT Landscape Modernization. American International Journal of Computer Science and Technology, 1(1), 23-27.
13. Gummadi, V. P. K. (2019). Microservices architecture with APIs: Design, implementation, and MuleSoft integration. Journal of Electrical Systems, 15(4), 130-134.
14. Garg, V. K., Soundappan, S. J., & Kaur, E. M. (2020). Enhancement in intrusion detection system for WLAN using genetic algorithms. South Asian Research Journal of Engineering and Technology, 2(6), 62–64. https://doi.org/10.36346/sarjet.2020.v02i06.003
15. Alex Roney Mathew. (2019). Malware analysis of API calls using FPGA hardware level security. International Journal for Research in Applied Science & Engineering Technology, 7(3), 898–900.
16. 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.
17. Anand, L., & Syed Ibrahim, S. P. (2018). HANN: a hybrid model for liver syndrome classification by feature assortment optimization. Journal of medical systems, 42(11), 211.
18. 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
19. Kotla, Mutha Ravi Tej (2022). Intelligent cloud-native banking: Leveraging machine learning for secure and scalable digital financial services. International Journal of Engineering and Technology Research, 7(1), 58–81. https://doi.org/10.34218/IJETR_07_01_005
20. Vayyasi, N. K. (2020). Decoding token volatility patterns with generative models deployed on cloud-native Java environments. International Journal of Engineering & Extended Technologies Research (IJEETR), 2(4), 1552–1565
21. Wadhwa, R. (2023). ENSURING DATA CONSISTENCY IN ENTERPRISE SYSTEMS THROUGH EVENT DRIVEN MICROSERVICES AND DISTRIBUTED TRANSACTION MANAGEMENT. International Journal of Computer Science and Engineering Research and Development, 6(1), 24-51.
22. Tasleem, N. A. Z. I. A., Gulati, D., & Sharma, S. (2023). Organizational readiness for change: A multi-dimensional framework. Iconic Research And Engineering Journals (IREJ), 1095-1108..
23. 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

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

||Volume 6, Issue 3, May-June 2023||

DOI:10.15662/IJRPETM.2023.0603007

24. Juvvadi, R. R. (2018). Continuous accounting: Toward a real-time financial reporting architecture for the modern enterprise. Computer Fraud & Security, 2018(12), 33–41.
25. 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.
26. Kavuri, S. (2022). Large Language Model (LLM)-Based Automation for Software Test Script Generation. Computer Fraud & Security, 17-28.
27. Shewale, V. (2022). Third-Party and Supply Chain Risk in Oil & Gas. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9596.
28. Lanka, S. (2022). Building smarter security systems with AI: Inside Citrix analytics for security. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(4), 93-109.
29. Parupalli, A., & Pandya, S. (2022). Compliance-Driven Data Governance: A Survey on GDPR, and HIPAA in Cloud Databases. vol, 12, 828-836.
30. NIST. (2020). Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5). National Institute of Standards and Technology.
31. Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
32. Stallings, W. (2018). Effective cybersecurity: A guide to using best practices and standards. Addison-Wesley.
33. Sweeney, L. (2002). k-Anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(5), 557–570.
34. Vaswani, A., et al. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30, 5998–6008.