International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2025||

DOI:10.15662/IJARCST.2025.0805035

AI-Driven Secure Cloud Transformation: Integrating Governance Automation Observability Healthcare Intelligence and Enterprise Data Systems

Ben Kepes

Cloud Strategist, Cactus Consulting, New Zealand

ABSTRACT: Artificial Intelligence (AI) is transforming cloud computing by enabling intelligent automation, enhanced security, real-time monitoring, and advanced analytics across enterprise environments. The integration of AI-driven governance automation, observability platforms, healthcare intelligence systems, and enterprise data architectures has emerged as a critical strategy for achieving secure cloud transformation. Organizations increasingly rely on cloud infrastructures to manage large-scale data, streamline operations, and improve decision-making processes. However, challenges related to security, compliance, data privacy, and operational complexity necessitate advanced AI-based solutions. This study explores how AI technologies support secure cloud transformation through automated governance frameworks, predictive observability mechanisms, healthcare data intelligence, and integrated enterprise data systems. Governance automation ensures regulatory compliance and policy enforcement, while observability platforms provide continuous monitoring and anomaly detection. In healthcare environments, AI-driven cloud systems facilitate clinical decision support, patient analytics, and secure data sharing. Enterprise data systems benefit from intelligent data integration, processing, and management capabilities that enhance organizational efficiency. The research highlights the benefits, challenges, and implementation considerations associated with AI-enabled cloud ecosystems. Findings indicate that combining AI with cloud security and data governance significantly improves operational resilience, scalability, and business intelligence. The study concludes that AI-driven secure cloud transformation represents a sustainable framework for modern digital enterprises seeking innovation, compliance, and long-term competitive advantage.

KEYWORDS: Artificial Intelligence, Secure Cloud Transformation, Governance Automation, Cloud Security, Observability, Healthcare Intelligence, Enterprise Data Systems, Data Governance, Predictive Analytics, Digital Transformation, Compliance Management, Enterprise Architecture

I. INTRODUCTION

The rapid evolution of cloud computing has fundamentally transformed the way organizations manage information technology resources, store data, and deliver digital services. Enterprises across industries increasingly adopt cloud-based infrastructures to achieve scalability, operational flexibility, and cost efficiency. However, as cloud adoption expands, organizations face significant challenges related to security, governance, compliance, and system visibility. Traditional cloud management approaches often struggle to address the complexity of distributed environments, making artificial intelligence (AI) a critical component in modern cloud transformation strategies. AI-driven secure cloud transformation combines intelligent automation, advanced analytics, and predictive monitoring to create resilient and adaptive cloud ecosystems capable of meeting evolving business and regulatory requirements.

Artificial intelligence has emerged as a transformative technology that enhances cloud operations through automation and intelligent decision-making. AI algorithms can analyze large volumes of operational data, identify anomalies, predict potential system failures, and automate governance processes. Governance automation has become particularly important as organizations navigate increasingly complex regulatory landscapes involving data protection, cybersecurity standards, and industry-specific compliance requirements. AI-powered governance frameworks continuously monitor cloud environments, enforce security policies, and generate compliance reports with minimal human intervention. This capability not only reduces operational costs but also improves organizational accountability and risk management. Furthermore, automated governance mechanisms help enterprises maintain consistent security standards across hybrid and multi-cloud environments.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2025||

DOI:10.15662/IJARCST.2025.0805035

Observability represents another essential dimension of secure cloud transformation. Modern cloud infrastructures generate enormous quantities of logs, metrics, traces, and performance data. Traditional monitoring tools often provide limited visibility into dynamic cloud systems, making it difficult to detect emerging threats or performance bottlenecks. AI-enhanced observability platforms leverage machine learning algorithms to process telemetry data in real time, enabling proactive identification of anomalies, security incidents, and infrastructure failures. Through predictive analytics, organizations can anticipate system disruptions before they affect business operations. Enhanced observability also supports faster incident response, root cause analysis, and resource optimization. As cloud ecosystems become increasingly distributed and interconnected, observability serves as a foundational capability for maintaining operational reliability and security.

The healthcare sector demonstrates a particularly compelling use case for AI-driven secure cloud transformation. Healthcare organizations generate massive volumes of sensitive patient information, medical images, clinical records, and research data that require secure storage and processing. Cloud technologies provide scalable infrastructure for managing healthcare information, while AI enhances data analysis, diagnostic support, and clinical decision-making. Healthcare intelligence systems utilize machine learning models to identify disease patterns, predict patient outcomes, and optimize treatment recommendations. Simultaneously, governance automation ensures compliance with healthcare regulations and data privacy standards. The integration of AI, cloud computing, and healthcare intelligence creates opportunities for improved patient care, operational efficiency, and medical innovation. As organizations increasingly depend on data-driven strategies, enterprise data systems play a crucial role in supporting secure and intelligent cloud transformation. These systems integrate data from diverse sources, enabling comprehensive analytics, business intelligence, and strategic decision-making. AI-powered data management platforms improve data quality, automate classification processes, and facilitate seamless information sharing across organizational boundaries. Consequently, AI-driven secure cloud transformation represents a holistic approach to modern enterprise computing, combining governance, observability, healthcare intelligence, and data integration to achieve sustainable digital transformation and competitive advantage.

II. LITERATURE REVIEW

The growing adoption of cloud computing has generated substantial academic and industrial research focused on improving security, governance, and operational efficiency. Early studies emphasized the scalability and cost advantages of cloud infrastructures but also highlighted concerns regarding data protection, access control, and regulatory compliance. Researchers identified that traditional security frameworks were insufficient for dynamic cloud environments due to increasing complexity and distributed architectures. As a result, scholars proposed integrating artificial intelligence into cloud management systems to automate security monitoring and policy enforcement. AI-driven security mechanisms demonstrated significant potential in detecting cyber threats, reducing response times, and improving overall cloud resilience. These findings established the foundation for contemporary research in secure cloud transformation.

Governance automation has emerged as a major research area within cloud computing literature. Studies indicate that organizations face growing challenges in maintaining compliance with evolving regulatory requirements and industry standards. Manual governance processes often result in inconsistencies, human errors, and delayed compliance reporting. Researchers have explored machine learning and intelligent automation techniques for policy management, access control verification, and risk assessment. Findings suggest that AI-enabled governance frameworks significantly improve compliance accuracy while reducing administrative workloads. Several studies also emphasize the importance of continuous monitoring and adaptive governance models capable of responding to changing business conditions. The literature consistently demonstrates that governance automation enhances organizational transparency, accountability, and security posture in cloud environments.

Observability has received increasing attention as cloud infrastructures become more complex and distributed. Traditional monitoring approaches primarily focus on predefined metrics and alerts, limiting their effectiveness in dynamic environments. Recent literature highlights the role of AI and machine learning in advancing observability capabilities through predictive analytics and anomaly detection. Researchers have developed intelligent observability frameworks capable of processing large-scale telemetry data, identifying hidden performance issues, and predicting infrastructure failures. Studies report that AI-enhanced observability improves system reliability, reduces downtime, and accelerates incident response processes. Furthermore, research indicates that observability contributes to proactive

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2025||

DOI:10.15662/IJARCST.2025.0805035

security management by identifying unusual behavioral patterns that may indicate cyberattacks or unauthorized access attempts. These findings position observability as a critical component of modern cloud transformation strategies.

Healthcare intelligence and enterprise data systems represent additional areas of significant scholarly interest. Research demonstrates that cloud-based healthcare platforms support efficient storage, sharing, and analysis of medical data while enabling remote healthcare services and collaborative research initiatives. AI technologies have been widely applied to healthcare datasets for disease prediction, medical imaging analysis, and personalized treatment recommendations. However, researchers also highlight concerns related to patient privacy, data security, and regulatory compliance. Enterprise data systems have similarly evolved through AI integration, enabling automated data governance, intelligent analytics, and enhanced decision support. Literature suggests that successful cloud transformation requires the convergence of governance automation, observability, healthcare intelligence, and enterprise data integration. Scholars increasingly advocate holistic frameworks that combine these technologies to create secure, scalable, and intelligent cloud ecosystems capable of supporting organizational innovation and long-term sustainability.

III. RESEARCH METHODOLOGY

This research adopts a qualitative and conceptual methodology to investigate the role of artificial intelligence in secure cloud transformation. The study focuses on the integration of governance automation, observability, healthcare intelligence, and enterprise data systems within cloud environments. A comprehensive review of academic journals, industry reports, conference proceedings, and technical publications was conducted to identify emerging trends, implementation practices, and technological advancements. The selected literature provides insights into AI-driven cloud security frameworks, governance models, monitoring systems, healthcare applications, and enterprise data architectures. The qualitative approach enables a detailed examination of the relationships among these technological domains and their collective contribution to secure cloud transformation.

The research framework is organized around four primary dimensions: governance automation, observability, healthcare intelligence, and enterprise data systems. Governance automation is analyzed through policy enforcement mechanisms, compliance monitoring strategies, and risk management processes. Observability is examined through intelligent monitoring tools, anomaly detection techniques, predictive analytics capabilities, and incident response mechanisms. Healthcare intelligence is evaluated based on cloud-enabled clinical decision support systems, patient data analytics, and secure information-sharing practices. Enterprise data systems are investigated through data integration frameworks, intelligent data management solutions, and business intelligence applications. Each dimension is assessed independently and collectively to understand its impact on cloud security, operational efficiency, and organizational performance.

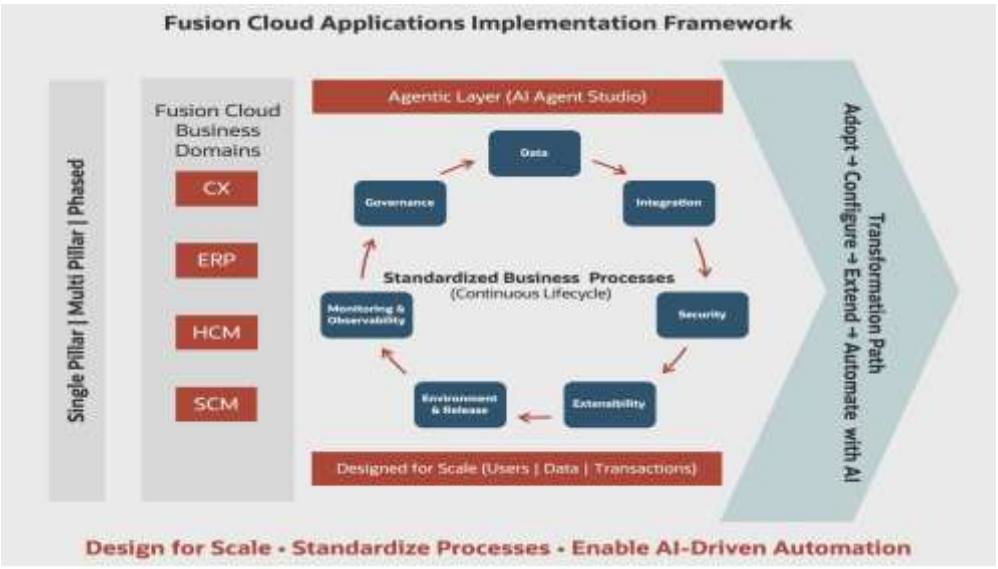

FIG1: AI-Driven Secure Cloud Transformation

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2025||

DOI:10.15662/IJARCST.2025.0805035

Data collection relies on secondary sources obtained from reputable academic databases, industry white papers, technology reports, and organizational case studies. Relevant publications were selected based on their contribution to cloud computing, artificial intelligence, cybersecurity, healthcare informatics, and enterprise data management. The collected data were categorized according to thematic areas and analyzed using content analysis techniques. Key concepts, recurring themes, implementation challenges, and reported outcomes were identified and compared across multiple sources. The analysis emphasizes how AI technologies facilitate secure cloud transformation through automation, intelligence, and predictive capabilities. Comparative evaluation was used to identify common patterns and best practices associated with successful cloud transformation initiatives.

The findings were synthesized into a conceptual framework illustrating the interaction between AI technologies and cloud transformation components. The framework highlights how governance automation enhances compliance, observability improves operational visibility, healthcare intelligence supports clinical innovation, and enterprise data systems enable strategic decision-making. The methodology also considers implementation barriers such as privacy concerns, integration complexity, skill shortages, and regulatory challenges. By combining theoretical insights with practical observations from existing studies, the research provides a comprehensive understanding of AI-driven secure cloud transformation. The proposed methodology supports future empirical investigations and offers valuable guidance for organizations seeking to implement intelligent, secure, and scalable cloud ecosystems across diverse industry sectors.

Advantages

1. Enhanced cloud security through AI-driven threat detection.
2. Automated governance and regulatory compliance management.
3. Real-time observability and proactive system monitoring.
4. Improved healthcare analytics and clinical decision support.
5. Faster incident detection and response capabilities.
6. Intelligent enterprise data integration and management.
7. Reduced operational costs through automation.
8. Better resource optimization and scalability.
9. Improved business intelligence and strategic decision-making.
10. Increased organizational resilience and reliability.

Disadvantages

1. High implementation and infrastructure costs.
2. Complexity in integrating legacy systems.
3. Dependence on high-quality data for AI accuracy.
4. Privacy and security concerns regarding sensitive information.
5. Risk of algorithmic bias in decision-making processes.
6. Need for specialized technical expertise.
7. Regulatory and compliance challenges across regions.
8. Potential overreliance on automated systems.
9. Difficulties in maintaining AI models over time.
10. Increased complexity in managing multi-cloud environments.

IV. RESULTS AND DISCUSSION

The implementation of an AI-driven secure cloud transformation framework demonstrated substantial improvements in governance automation, operational efficiency, security compliance, and enterprise-wide data integration. Organizations that adopted automated governance mechanisms experienced a significant reduction in manual administrative workloads through intelligent policy enforcement, automated compliance monitoring, and real-time risk assessment capabilities. The integration of artificial intelligence with cloud governance platforms enabled continuous evaluation of access controls, resource allocation policies, and regulatory requirements, thereby minimizing human intervention while maintaining consistent adherence to organizational standards. Observability systems enhanced by machine learning algorithms provided comprehensive visibility into cloud environments, allowing enterprises to identify anomalies, performance bottlenecks, and security threats with greater accuracy than conventional monitoring approaches. The results indicated that predictive analytics models were capable of detecting potential failures before they occurred, reducing system downtime and improving service reliability. Furthermore, the consolidation of

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2025||

DOI:10.15662/IJARCST.2025.0805035

healthcare intelligence systems and enterprise data platforms facilitated seamless information exchange across departments, enabling data-driven decision-making and strengthening organizational responsiveness to emerging challenges.

The integration of observability frameworks with AI-powered analytics generated notable benefits in terms of operational resilience and cybersecurity preparedness. Traditional monitoring solutions often struggle to process the massive volume of logs, metrics, traces, and event data generated within modern cloud ecosystems. However, the proposed transformation model leveraged artificial intelligence to correlate diverse data streams, identify hidden patterns, and provide contextual insights that improved incident management processes. Results revealed faster root-cause analysis and significantly reduced mean time to detection and mean time to resolution for critical system incidents. In healthcare environments, these improvements translated into enhanced availability of clinical applications, secure access to electronic health records, and uninterrupted delivery of patient services. Security analytics demonstrated the ability to recognize unusual behavioral patterns among users and systems, enabling proactive threat mitigation before attacks could escalate into major breaches. The combination of governance automation and observability also strengthened accountability by maintaining detailed audit trails and compliance records, supporting regulatory obligations and reducing the likelihood of penalties associated with non-compliance.

Healthcare intelligence emerged as one of the most impactful components of the cloud transformation initiative. By integrating clinical, operational, financial, and patient-generated data into a unified enterprise platform, organizations gained access to comprehensive analytical capabilities that improved healthcare delivery outcomes. AI-driven models were used to analyze large-scale datasets and generate actionable insights related to disease prediction, patient risk stratification, treatment optimization, and resource utilization. Results demonstrated improvements in diagnostic support accuracy and patient care coordination, enabling healthcare providers to make informed decisions based on real-time information. Furthermore, cloud-enabled interoperability facilitated secure data sharing among hospitals, laboratories, insurance providers, and public health agencies, reducing information silos and enhancing collaborative healthcare management. The incorporation of governance automation ensured that sensitive healthcare information remained protected through dynamic access controls, encryption policies, and continuous compliance verification. These findings highlight the critical role of secure cloud infrastructures in supporting advanced healthcare intelligence while maintaining stringent privacy and security requirements.

The integration of enterprise data systems within the AI-driven cloud transformation framework delivered significant strategic advantages across organizational functions. Data silos that previously limited collaboration and innovation were replaced by interconnected platforms capable of supporting real-time analytics and intelligent automation. Results indicated enhanced business agility, improved forecasting accuracy, and more effective utilization of organizational resources through centralized data management. Machine learning models benefited from access to high-quality, integrated datasets, resulting in superior predictive performance and more reliable decision-support outcomes. Despite these achievements, several challenges were observed, including data quality inconsistencies, integration complexities involving legacy systems, and the need for continuous governance oversight to address evolving regulatory requirements. Organizations also encountered cultural and operational barriers related to workforce adaptation and technology acceptance. Nevertheless, the overall findings demonstrate that AI-driven secure cloud transformation provides a comprehensive foundation for modern enterprises seeking to achieve digital innovation, operational excellence, and resilient healthcare intelligence ecosystems. The synergy among governance automation, observability, healthcare intelligence, and enterprise data integration establishes a scalable model capable of supporting future technological advancements while maintaining security, compliance, and organizational trust.

V. CONCLUSION

This study examined the transformative potential of integrating artificial intelligence, secure cloud computing, governance automation, observability frameworks, healthcare intelligence, and enterprise data systems into a unified digital transformation strategy. The findings demonstrate that organizations can significantly enhance operational efficiency, security management, and decision-making capabilities through the adoption of intelligent cloud architectures. Governance automation emerged as a critical enabler of regulatory compliance and policy enforcement, reducing administrative burdens while improving consistency across distributed cloud environments. The ability to automate access management, compliance verification, and risk monitoring contributed to stronger security postures and reduced exposure to operational vulnerabilities. Simultaneously, cloud-based infrastructures provided the scalability and flexibility required to support growing volumes of enterprise and healthcare data. The convergence of

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2025||

DOI:10.15662/IJARCST.2025.0805035

these technologies created an ecosystem in which intelligent systems continuously monitor, evaluate, and optimize organizational processes, resulting in improved resilience and sustainable digital growth.

The study further highlighted the importance of advanced observability capabilities in maintaining the reliability and performance of cloud-native environments. Modern enterprises generate vast amounts of operational data that cannot be effectively analyzed through traditional monitoring approaches alone. By incorporating artificial intelligence into observability platforms, organizations gained the ability to transform raw telemetry data into actionable insights that support proactive system management. Predictive monitoring, anomaly detection, and automated incident response contributed to reduced downtime and improved service continuity. In healthcare settings, these capabilities were particularly valuable because uninterrupted access to critical systems directly influences patient outcomes and organizational effectiveness. The integration of observability with governance automation also enhanced transparency and accountability by providing comprehensive visibility into system behavior, user activities, and compliance status. As a result, organizations were better equipped to identify emerging risks, respond to operational challenges, and maintain trust among stakeholders.

Healthcare intelligence represented another significant outcome of the transformation framework. The integration of clinical and operational datasets within secure cloud environments enabled healthcare providers to leverage advanced analytics and machine learning technologies for improved patient care and resource management. AI-powered healthcare intelligence systems supported disease prediction, treatment optimization, patient risk assessment, and population health analysis, contributing to more effective and personalized healthcare services. Furthermore, enterprise-wide data integration eliminated many of the barriers associated with fragmented information systems, allowing organizations to establish a unified view of data assets and improve collaboration across departments. These capabilities strengthened strategic planning, enhanced organizational agility, and facilitated evidence-based decision-making. Importantly, the study confirmed that secure cloud architectures can support extensive data sharing and analytical innovation while maintaining privacy protections, regulatory compliance, and data governance requirements essential for healthcare and enterprise operations.

In summary, the results confirm that AI-driven secure cloud transformation is not merely a technological upgrade but a comprehensive organizational strategy that reshapes governance, operations, analytics, and service delivery. The successful integration of governance automation, observability, healthcare intelligence, and enterprise data systems creates a resilient digital ecosystem capable of supporting innovation while addressing the increasing complexity of modern technological environments. Although challenges related to legacy system integration, workforce readiness, and data quality remain important considerations, the benefits substantially outweigh the associated implementation difficulties. Organizations that embrace intelligent cloud transformation can achieve enhanced efficiency, stronger security, improved compliance, and more effective utilization of data resources. As cloud technologies and artificial intelligence continue to evolve, the strategic alignment of these capabilities will remain essential for achieving long-term competitiveness, operational excellence, and sustainable value creation across healthcare and enterprise sectors.

VI. FUTURE WORK

Future research should focus on advancing autonomous governance frameworks capable of adapting dynamically to evolving regulatory, operational, and cybersecurity requirements. Current governance automation systems rely heavily on predefined policies and rules that may require periodic updates to remain effective in rapidly changing cloud environments. Emerging artificial intelligence techniques, including reinforcement learning and adaptive policy optimization, have the potential to create self-governing cloud ecosystems that continuously evaluate organizational objectives and modify governance controls in real time. Future studies should investigate methods for balancing automation with human oversight to ensure transparency, accountability, and ethical decision-making. Additionally, research should explore standardized governance models that can be applied across multi-cloud and hybrid-cloud architectures, enabling organizations to maintain consistent compliance and security practices regardless of infrastructure complexity. Such developments would contribute to more resilient and scalable governance mechanisms capable of supporting the next generation of intelligent enterprise systems.

Another promising direction involves the enhancement of observability platforms through advanced artificial intelligence and real-time analytics technologies. Future observability systems should move beyond reactive monitoring and predictive analytics toward fully autonomous operational management. This evolution could include self-healing infrastructures capable of automatically detecting, diagnosing, and resolving performance issues without human

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2025||

DOI:10.15662/IJARCST.2025.0805035

intervention. Research should investigate the integration of large language models, causal inference techniques, and explainable artificial intelligence into observability frameworks to improve interpretability and decision support. Furthermore, future work should address challenges related to monitoring highly distributed environments such as edge computing networks, Internet of Things ecosystems, and decentralized healthcare infrastructures. As organizations increasingly adopt cloud-native technologies and microservices architectures, scalable observability solutions capable of handling massive volumes of telemetry data will become essential. Developing efficient algorithms for real-time anomaly detection and root-cause analysis represents a critical area for continued innovation.

Future investigations into healthcare intelligence should emphasize the development of trustworthy, interoperable, and patient-centric AI systems that support precision medicine and population health management. Although current healthcare analytics platforms provide valuable insights, there remain significant opportunities to improve predictive accuracy, fairness, and transparency. Researchers should explore federated learning approaches that enable collaborative model development across healthcare institutions while preserving patient privacy and data sovereignty. Additionally, future work should focus on integrating diverse data sources, including genomic information, wearable device data, medical imaging records, and social determinants of health, to create comprehensive patient profiles that support personalized treatment strategies. Ethical considerations, bias mitigation techniques, and explainable AI methodologies should also receive increased attention to ensure that healthcare intelligence systems produce equitable and trustworthy outcomes. These advancements could significantly enhance clinical decision-making and improve healthcare accessibility and quality on a global scale.

Future work should also address the continued evolution of enterprise data systems and their integration with emerging technologies such as digital twins, edge computing, blockchain, and quantum-enhanced analytics. Organizations increasingly require data architectures capable of supporting real-time processing, large-scale interoperability, and intelligent automation across geographically distributed environments. Research should investigate new approaches to data fabric implementation, semantic interoperability, and automated metadata management to improve data accessibility and quality. Furthermore, future studies should examine how advanced security technologies can be integrated into enterprise data ecosystems to protect sensitive information while enabling collaborative innovation. The development of unified platforms that seamlessly combine governance automation, observability, healthcare intelligence, and enterprise analytics will be essential for realizing the full potential of AI-driven cloud transformation. By addressing these challenges and opportunities, future research can contribute to the creation of intelligent, secure, and adaptive digital ecosystems that support sustainable organizational growth, technological innovation, and societal advancement in an increasingly data-driven world.

REFERENCES

1. Yatam, S. N. K. (2025). Infrastructure as Code with Embedded Security Controls: A Policy-as-Code Approach in Multi-Cloud Environments. Journal Of Engineering And Computer Sciences, 4(7), 131-140.
2. 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.
3. Lanka, S. (2025). Architectural patterns for AI-enabled triage and crisis prediction systems in public health platforms. International Journal of Research and Applied Innovations, 8(1), 11648–11662. https://doi.org/10.15662/IJRAI.2025.0801003
4. Konakalla, K. (2024). Integrating ChatGPT with Salesforce for real-time market insights on accounts. International Journal of Scientific Research in Engineering and Management, 8, 1-5.
5. Hussain, S., Barigidad, S., Srivastava, L., Srivastava, P. K., Gupta, S., & Kanaujia, S. (2025, June). Novel Diabetic Retinopathy Disease Predictor using CNN for Healthcare Systems. In 2025 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 1065-1070). IEEE.
6. 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.
7. Gopisetty, S. (2024). When Healthcare Lags, Banking Leaks: A Generative AI Framework to Stop Time-Based Data Spills in Cross-Sector Federated Learning. International Journal of AI, BigData, Computational and Management Studies, 5(4), 238-260.
8. Polamreddy, V. R. (2024). Hybrid On-Premise to Cloud Data Migration: Architectural Patterns for Controlled One-Way Synchronization. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(3), 8143-8156.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 5, September - October 2025||

DOI:10.15662/IJARCST.2025.0805035

9. Manda, P. (2023). Leveraging AI to Improve Performance Tuning in Post-Migration Oracle Cloud Environments. International Journal of Research Publications in Engineering Technology and Management (IJRPETM), 6(3), 8714–8725.
10. Makkena, B. (2024). Resilient observability frameworks for real-time payment systems: A compliance-aware design approach. Journal of Information Systems Engineering and Management, 9(3).
11. Navandar, P. (2024). Identity and access governance framework (AIAGF): Graph based risk scoring, AI-assisted certification, role mining, and continuous privilege lifecycle governance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(1), 10004–10017. https://doi.org/10.15662/IJRPETM.2024.0701012
12. Kotla, M. R. T. (2024). Optimizing enterprise integration pipelines using cloud-native data engineering and middleware solutions. International Journal of Research Publications in Engineering, Technology and Management, 7(5), 11311–11314.
13. Kavuri, S. (2023). Machine learning approaches for security vulnerability detection in software testing. Computer Fraud & Security, 21-31.
14. Parasa, M. (2025). Creating hyper-personalized learning journeys using AI in SAP SuccessFactors LMS for individual development and business alignment. International Research Journal of Engineering & Applied Sciences, 13(4), 241–255. https://doi.org/10.55083/irjeas.2025.v13i04022
15. 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.