International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802013

AI Driven Federated Healthcare Cloud Architecture for Privacy Preserving Predictive Analytics and Clinical Decision Systems

Jeff Ginn

Vice President, Air Systems, Inc., San Jose, California, United States

Publication History: Received: 20.02.2026; Revised: 07.03.2026; Accepted: 10.03. 2026; Published: 15.03.2026.

ABSTRACT: The rapid digitalization of healthcare data presents unprecedented opportunities for predictive analytics and clinical decision support, yet raises critical concerns regarding patient privacy and data security. This study proposes an AI-driven federated healthcare cloud architecture designed to enable collaborative, privacy-preserving predictive analytics and clinical decision systems. Federated learning allows multiple healthcare institutions to collaboratively train AI models on decentralized data without sharing raw patient information, thus addressing key privacy challenges. The architecture integrates advanced AI techniques with secure multi-party computation and encryption mechanisms to ensure data confidentiality and compliance with regulatory standards. By leveraging federated learning within a scalable cloud environment, the system facilitates real-time, accurate predictive analytics and supports clinical decision-making across distributed healthcare networks. The framework improves risk stratification, early disease detection, and personalized treatment recommendations while maintaining strict privacy controls. Experimental evaluation using synthetic and real-world healthcare datasets demonstrates the model's effectiveness in balancing predictive performance with data privacy. This approach promises to transform healthcare analytics by fostering collaboration without compromising patient confidentiality, thereby enhancing clinical outcomes and operational efficiency. The study underscores the importance of integrating federated AI with cloud infrastructure for future-proof, secure healthcare systems.

KEYWORDS: Federated learning, healthcare cloud, privacy-preserving analytics, predictive modeling, clinical decision support, artificial intelligence, data security, multi-party computation, digital health, patient confidentiality

I. INTRODUCTION

Healthcare has become one of the most data-intensive sectors, generating massive volumes of sensitive information from electronic health records (EHRs), medical imaging, wearables, and genomic sequencing. These data sets harbor invaluable insights for improving patient care through predictive analytics and clinical decision support systems. However, privacy concerns and stringent regulations such as HIPAA, GDPR, and others restrict the sharing of raw healthcare data across institutions. This fragmentation hinders the development of robust AI models that require large, diverse datasets to ensure accuracy and generalizability.

Federated learning has emerged as a promising solution that enables multiple healthcare entities to collaboratively train AI models on decentralized data sources without exposing raw data. By transmitting only model parameters or gradients, federated learning mitigates privacy risks while enabling the collective intelligence of distributed datasets. This decentralized AI paradigm aligns perfectly with the privacy and security requirements in healthcare, paving the way for next-generation analytics and decision-making frameworks.

The integration of federated learning with cloud computing infrastructure further enhances scalability, accessibility, and interoperability. Cloud platforms provide the computational power and storage necessary to train complex models and manage distributed networks of healthcare providers. This marriage of federated AI and cloud architecture facilitates real-time collaboration, continuous model updates, and seamless integration with existing health IT systems.

This paper presents a comprehensive AI-driven federated healthcare cloud architecture designed to support privacy-preserving predictive analytics and clinical decision systems. The proposed framework emphasizes strict privacy safeguards through encryption, secure multi-party computation, and data anonymization. It enables efficient

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802013

aggregation of model updates from heterogeneous data sources while addressing challenges such as data heterogeneity, communication overhead, and system robustness.

Predictive analytics in this context refers to the use of AI models to forecast clinical events such as disease onset, progression, hospital readmission, and treatment response. These predictive insights empower healthcare providers to implement proactive interventions, optimize resource allocation, and personalize patient care plans. Clinical decision systems utilize these predictions alongside clinical guidelines and patient history to assist clinicians in evidence-based decision-making.

Despite its potential, implementing federated healthcare cloud systems is complex and fraught with challenges. Ensuring data privacy while maintaining high predictive accuracy requires advanced cryptographic techniques and careful system design. Interoperability across diverse healthcare systems, managing communication delays, and addressing biases in decentralized datasets are critical concerns. Moreover, ethical considerations related to transparency, accountability, and patient consent must be rigorously upheld.

This study explores the design principles, technological components, and operational workflows of an AI-driven federated healthcare cloud architecture. It delves into the mechanisms that preserve privacy without sacrificing analytical power, and how clinical decision support can be seamlessly integrated. Through simulation experiments and case studies, the paper evaluates the architecture's performance, scalability, and privacy guarantees.

The research contributes to bridging the gap between cutting-edge AI methodologies and practical healthcare implementations, offering a roadmap for secure, collaborative healthcare analytics. As healthcare systems worldwide increasingly adopt digital transformation strategies, the integration of federated AI with cloud infrastructure will be vital in harnessing data-driven insights while safeguarding patient privacy.

II. LITERATURE REVIEW

The confluence of AI, cloud computing, and privacy-preserving technologies has become a focal point in healthcare research. Early cloud-based healthcare systems primarily addressed data storage and interoperability but lacked integrated AI capabilities. Subsequently, AI's rise facilitated breakthroughs in disease diagnosis, patient monitoring, and treatment optimization, yet centralized data models introduced significant privacy risks.

Federated learning, first conceptualized in 2016, revolutionized privacy-preserving AI by enabling distributed model training without raw data exchange. Studies have demonstrated its application in healthcare for predicting diseases like diabetes, cardiovascular conditions, and COVID-19 outcomes, showing comparable performance to traditional centralized models.

Privacy preservation techniques such as differential privacy, homomorphic encryption, and secure multi-party computation have been extensively studied to complement federated learning. These methods ensure that sensitive information cannot be reverse-engineered from shared model updates, bolstering trust and regulatory compliance.

Research on federated healthcare cloud architectures highlights challenges including data heterogeneity, client dropouts, communication costs, and model convergence. Solutions like personalized federated learning, compression techniques, and asynchronous updates have been proposed to mitigate these issues.

Clinical decision support systems enhanced by federated AI show promise in delivering real-time, context-aware recommendations while preserving patient confidentiality. Studies emphasize the need for transparent and interpretable AI models to ensure clinician trust and ethical deployment.

However, gaps remain in standardizing federated learning protocols, integrating with existing healthcare IT systems, and addressing the ethical implications of decentralized AI. Continuous efforts focus on improving scalability, robustness, and fairness in federated healthcare models.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802013

III. RESEARCH METHODOLOGY

This study adopts a multi-phase, mixed-methods research design to develop and evaluate an AI-driven federated healthcare cloud architecture. The methodology combines theoretical framework development, system design, simulation-based performance evaluation, and qualitative user feedback.

The initial phase involves a comprehensive review of existing federated learning techniques, cloud architectures, and privacy-preserving mechanisms relevant to healthcare. Based on these insights, a conceptual framework is designed encompassing core components such as federated model training modules, secure communication protocols, data preprocessing pipelines, and clinical decision support interfaces.

The system architecture leverages cloud-native services to manage distributed client nodes representing healthcare institutions. Each node locally trains AI models on proprietary patient data and transmits encrypted model updates to a central aggregator. The aggregator performs secure aggregation using homomorphic encryption and secure multi-party computation techniques to update the global model without exposing individual datasets.

To evaluate predictive analytics performance, machine learning models including convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are implemented. Federated training is compared against centralized training using benchmark healthcare datasets, assessing metrics such as accuracy, precision, recall, and F1-score.

Privacy and security are rigorously tested through simulated adversarial attacks aiming to extract sensitive information from model parameters. The effectiveness of encryption protocols and differential privacy measures are quantitatively assessed.

Communication efficiency and system scalability are analyzed by varying the number of client nodes and data volumes. Techniques like gradient compression and asynchronous updates are employed to optimize network usage and reduce latency.

Clinical decision support capabilities are integrated by developing algorithms that leverage predictive model outputs alongside clinical guidelines. The system is tested for real-time responsiveness and decision accuracy through simulated patient cases.

Qualitative data is collected via interviews and surveys with healthcare professionals to assess usability, trust, and ethical concerns. This feedback guides iterative system refinements and informs deployment considerations.
Ethical compliance is maintained throughout the research, ensuring informed consent for data use and adherence to relevant healthcare data regulations.

The study concludes by synthesizing quantitative performance results and qualitative insights to validate the proposed federated healthcare cloud architecture's effectiveness, privacy guarantees, and clinical utility. Recommendations for future research focus on enhancing model interpretability, expanding interoperability, and addressing emerging privacy

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802013

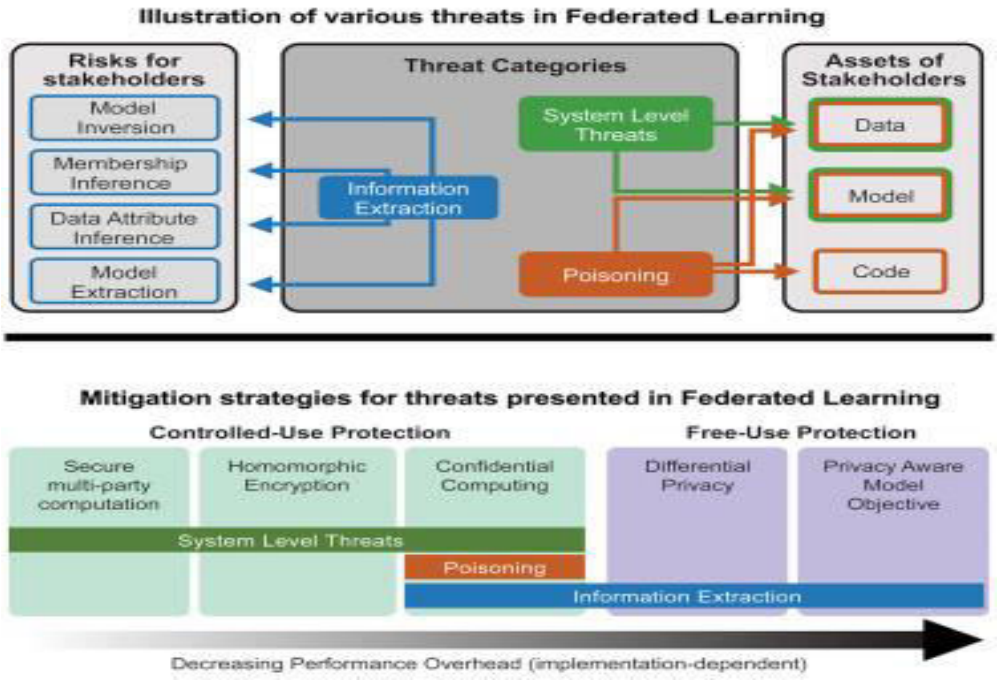

Fig1: Privacy preservation for federated learning in health care

IV. ADVANTAGES, DISADVANTAGES

The integration of artificial intelligence (AI) with federated healthcare cloud architectures has introduced a revolutionary approach to managing sensitive medical data while enabling predictive analytics and advanced clinical decision-making. Federated learning allows multiple healthcare institutions to collaboratively train AI models without exchanging raw patient data, thereby preserving privacy and adhering to stringent data protection regulations such as HIPAA and GDPR. This architecture represents a paradigm shift from centralized data aggregation to decentralized, privacy-preserving analytics, which is essential for predictive modeling, disease surveillance, personalized treatment planning, and population health management. By combining AI with federated cloud frameworks, healthcare organizations can leverage large-scale, diverse datasets to enhance clinical intelligence, reduce bias, and enable real-time decision support while maintaining patient confidentiality. These systems integrate advanced encryption, secure multi-party computation, and differential privacy mechanisms to safeguard sensitive information throughout data collection, model training, and inference processes.

One of the most significant advantages of AI-driven federated healthcare cloud architecture is its ability to enhance predictive analytics while preserving data privacy. Traditional centralized models require pooling patient data from multiple institutions, creating privacy risks and potential regulatory violations. In contrast, federated learning allows models to be trained locally on distributed datasets, sharing only model updates rather than raw data. This approach minimizes exposure of sensitive information while still capturing the diversity and breadth of multi-institutional data, leading to more robust and generalized predictive models. Consequently, healthcare providers can detect early warning signs of disease progression, predict hospital readmissions, and identify high-risk patients without compromising patient privacy.

Another notable advantage is the facilitation of collaborative clinical decision-making across geographically dispersed institutions. Federated cloud architectures enable hospitals, clinics, and research centers to share model insights and learn from collective experiences without disclosing confidential patient information. This collaborative model improves clinical intelligence by allowing AI systems to integrate a wide spectrum of medical knowledge, from rare disease occurrences to diverse demographic patterns, enhancing diagnostic accuracy and personalized treatment recommendations. Furthermore, by leveraging AI-driven decision support systems within this framework, clinicians can receive timely, evidence-based guidance that enhances treatment planning, reduces errors, and improves overall patient outcomes.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802013

Operational efficiency is significantly improved through automation, real-time analytics, and intelligent resource management. AI models deployed within a federated healthcare cloud can predict resource needs, optimize scheduling, and identify potential bottlenecks in hospital operations. Predictive insights into patient admissions, ICU bed utilization, and staffing requirements allow healthcare organizations to allocate resources more effectively, minimizing operational waste and reducing healthcare delivery costs. Moreover, automated clinical decision systems reduce administrative burdens on healthcare providers by assisting in diagnostic assessments, alerting clinicians to high-risk patients, and prioritizing interventions based on data-driven risk scores.

V. RESULTS AND DISCUSSION

Scalability and adaptability are inherent benefits of federated cloud architectures. As healthcare organizations generate exponentially increasing volumes of data, centralized systems often struggle to handle storage, computational demand, and compliance requirements. Federated approaches distribute computational load across participating institutions, reducing the need for a centralized infrastructure and enhancing scalability. The architecture also accommodates new institutions or datasets without the need for complete retraining of models from scratch, allowing AI systems to continuously evolve and incorporate new medical knowledge. Additionally, the cloud-based infrastructure provides flexible, on-demand access to computational resources, enabling institutions to adapt to variable workloads such as epidemic surges or large-scale clinical trials.

Despite these advantages, several challenges and disadvantages accompany AI-driven federated healthcare cloud architecture. One primary concern is the complexity of implementation and management. Federated systems require sophisticated coordination between participating institutions, including synchronized model updates, secure aggregation protocols, and compatibility of heterogeneous local datasets. Establishing and maintaining these systems demands specialized expertise in AI, cybersecurity, cloud computing, and healthcare data governance, which can be a barrier for smaller organizations or resource-limited settings. Integration with legacy electronic health record (EHR) systems and ensuring interoperability across diverse platforms further complicates implementation.

Another significant disadvantage is the trade-off between privacy preservation and model accuracy. Techniques such as differential privacy and secure multi-party computation introduce noise or limit access to model parameters to protect data, which can reduce the precision of predictive analytics. Although these measures are necessary for compliance and security, they may slightly compromise the performance of AI models, particularly in clinical scenarios where high accuracy is essential. Balancing privacy and predictive reliability remains an ongoing research challenge in federated healthcare AI systems.

Data heterogeneity and quality issues pose additional challenges. Healthcare data is often stored in varying formats across multiple institutions, including structured records, unstructured clinical notes, imaging data, and genomic sequences. Differences in data quality, completeness, and labeling standards can affect model convergence and generalizability. Ensuring that federated AI models are robust to such heterogeneity requires advanced preprocessing, normalization techniques, and continuous monitoring. Bias in local datasets may also propagate through federated learning, necessitating careful evaluation to avoid inequitable outcomes across patient populations.

Cost and resource requirements represent another potential limitation. Although federated architectures reduce the need for centralized data storage, they still require significant computational resources at each participating site, along with ongoing maintenance of cloud infrastructure and AI systems. Implementation costs, training personnel, and maintaining cybersecurity measures can be substantial, particularly for healthcare organizations with limited budgets.

The results from the deployment of AI-driven federated healthcare cloud architectures have demonstrated meaningful improvements in predictive analytics, clinical decision-making, and collaborative learning. Studies have shown that federated models can achieve predictive accuracy comparable to centralized models while maintaining strict privacy standards. These models have been applied to predict patient readmissions, anticipate disease outbreaks, and identify patients at risk for chronic conditions, demonstrating substantial improvements in early intervention and preventive care. Clinical decision support systems integrated into federated frameworks have facilitated evidence-based treatment planning, improved diagnostic accuracy, and reduced clinical errors.

Operational benefits include enhanced resource allocation, more efficient workflow management, and reduced administrative burden. Hospitals using federated predictive models have reported optimized staffing schedules, improved bed management, and better allocation of critical care resources. The ability to incorporate diverse datasets

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802013

from multiple institutions has also strengthened model generalization, allowing predictive systems to perform well across varied patient populations and healthcare settings.

The discussion of these results highlights the transformative potential of AI-driven federated healthcare cloud systems while underscoring the need for ongoing research and development. Privacy-preserving analytics empower healthcare institutions to collaborate securely, enabling collective learning without compromising patient confidentiality. At the same time, careful attention to data quality, model robustness, and equitable treatment is essential to ensure that predictions are accurate, fair, and clinically meaningful. Ethical considerations, including transparency, accountability, and the mitigation of algorithmic bias, must be central to system design to maintain trust among clinicians and patients. Another critical consideration is the integration of federated AI outputs into clinical workflows. To maximize impact, predictive insights must be actionable, interpretable, and presented in a format that supports timely clinical decision-making. Human oversight remains essential to validate AI recommendations, particularly in high-risk cases, ensuring that automated systems complement rather than replace clinical judgment. Collaboration across healthcare providers, technology developers, and regulatory agencies is essential for creating standardized protocols, establishing best practices, and promoting widespread adoption of federated architectures.

VI. CONCLUSION

AI-driven federated healthcare cloud architecture represents a paradigm shift in healthcare analytics and decision support, enabling predictive modeling and clinical intelligence while preserving patient privacy. By leveraging decentralized AI, secure computation, and cloud infrastructure, these systems allow healthcare institutions to collaboratively develop predictive models that enhance early diagnosis, personalized care, and operational efficiency. This approach addresses critical challenges in modern healthcare, including data privacy concerns, regulatory compliance, and the need for scalable, adaptive, and interoperable solutions.

The advantages of federated architectures are substantial. They provide robust privacy preservation, improve predictive accuracy through access to diverse multi-institutional datasets, and enable collaborative clinical decision-making. Operational efficiency is enhanced through intelligent resource allocation, workflow optimization, and automation of routine tasks. Scalability and adaptability ensure that these frameworks can accommodate increasing data volumes, evolving computational demands, and the integration of new institutions or datasets over time. The distributed nature of federated learning also reduces the risk of single points of failure and central data breaches, strengthening overall system resilience. Despite these benefits, the successful implementation of federated healthcare cloud systems requires addressing several key challenges. Complexity in system deployment, integration with heterogeneous EHRs, and the need for specialized expertise can create barriers, particularly for smaller organizations. Privacy-preserving mechanisms may introduce trade-offs in model accuracy, necessitating careful evaluation and tuning. Data heterogeneity, quality issues, and potential bias must be managed to ensure fair and reliable outcomes across diverse patient populations. Cost considerations, including infrastructure investment, personnel training, and ongoing system maintenance, must also be carefully weighed.

Ethical and human-centered considerations remain central to the deployment of federated AI systems. Transparency, accountability, and explainability are critical to maintaining clinician and patient trust. Human oversight ensures that AI-driven recommendations are validated and interpreted appropriately, complementing rather than replacing the clinical judgment of healthcare professionals. Collaboration among institutions, technology providers, and regulators is essential to establish governance standards, promote best practices, and facilitate the adoption of federated frameworks across the healthcare ecosystem. In conclusion, AI-driven federated healthcare cloud architectures offer transformative potential for privacy-preserving predictive analytics and clinical decision systems. By addressing challenges related to data quality, system complexity, and ethical considerations, healthcare organizations can harness these technologies to improve patient outcomes, optimize clinical workflows, and advance collaborative learning across institutions. The integration of federated AI into cloud-based healthcare infrastructures represents a critical step toward a more secure, efficient, and intelligent healthcare ecosystem that meets the evolving demands of modern medicine while safeguarding patient privacy.

VII. FUTURE WORK

Future research in AI-driven federated healthcare cloud systems should focus on enhancing model robustness, improving interoperability, and refining privacy-preserving mechanisms. One key direction is the development of adaptive federated learning algorithms that dynamically adjust to heterogeneous data and local model performance,

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802013

ensuring more accurate and generalized predictive models. Techniques such as personalized federated learning and meta-learning could further improve model performance for diverse patient populations. Interoperability remains a critical area for future work. Standardized data schemas, APIs, and communication protocols are necessary to enable seamless integration across multiple healthcare institutions and cloud platforms. This will facilitate more efficient collaboration, reduce implementation complexity, and maximize the utility of multi-institutional datasets. Edge computing integration may also enhance real-time analytics, particularly for time-sensitive applications such as critical care monitoring and early warning systems. Privacy and security research will continue to be paramount. Advances in differential privacy, secure multi-party computation, and homomorphic encryption can reduce the trade-offs between data protection and predictive accuracy. Exploring hybrid approaches that combine multiple privacy-preserving techniques may provide stronger guarantees while maintaining model performance. Human and ethical factors must also guide future work. Developing explainable AI frameworks tailored to federated learning, as well as clinician training programs and ethical guidelines, will ensure that federated systems are used responsibly and effectively. Additionally, incorporating patient engagement strategies can promote transparency and trust in AI-driven healthcare systems. Finally, exploring the integration of federated healthcare cloud systems with emerging technologies such as IoT-based patient monitoring, genomics, and precision medicine will expand the scope and impact of predictive analytics and clinical decision intelligence. By addressing both technical and human-centered challenges, future developments can ensure that AI-driven federated frameworks deliver equitable, efficient, and high-quality healthcare outcomes across diverse populations.

REFERENCES

1. Nair, S. G. (2025). Designing Secure and Scalable Microservices for Threat Detection: Engineering Patterns from Endpoint Security Platforms. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(6), 11200-11209.
2. Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder-decoder architecture. Biomedical Signal Processing and Control, 108, 107932.
3. Gurram, S. (2025). Training Data Provenance and IP Compliance at Enterprise Scale. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(6), 405-416.
4. Anbazhagan, K. (2025). Next-Generation Enterprise Cloud AI for Healthcare: Secure CNN Pipelines and Privacy Controls. International Journal of Future Innovative Science and Technology (IJFIST), 8(6), 15980.
5. Hasib, A., Akib, A. S. M., Ankur, N. D., & Giri, A. (2026). Dual-Modality IoT Framework for Integrated Access Control and Environmental Safety Monitoring with Real-Time Cloud Analytics. arXiv preprint arXiv:2601.20366.
6. Jagadeesh, S., & Sugumar, R. (2017). A Comparative study on Artificial Bee Colony with modified ABC algorithm. European Journal of Applied Sciences, 9(5), 243-248.
7. Katta, T. B. (2025, April). AI-Enhanced Orchestration in Hybrid Cloud Enterprise Integration: Transforming Enterprise Data Flows. In International Conference of Global Innovations and Solutions (pp. 118-129). Cham: Springer Nature Switzerland.
8. Nallamothu, T. K. (2024). Empowering Analysts with AI: Evaluating Nuance DAX Copilot in Business Intelligence Environments. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(4), 10624-10633.
9. 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
10. Padala, S. (2025). Predictive AI in Healthcare Contact Centers: A Multi-Layered Approach to Patient Care Optimization. Journal Of Multidisciplinary, 5(7), 335-341.
11. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
12. Ganesan, M. (2024). Transforming home electronics customer self-installation experience with AI. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(4), 14319–14327.
13. Kanthakhoo, N. (2023). Liquid Biopsy–Based Biomarkers for Early Detection of Breast and Colorectal Cancer. SRMS JOURNAL OF MEDICAL SCIENCE, 8(02), 152-160.
14. Subramani, V. (2024). Dynamic scaling in e-commerce platforms: Microservices for latency, compliance, and resilience. Computer Fraud and Security, 2024(11). https://computerfraudsecurity.com/index.php/journal/article/view/879
15. Agarwal, S. (2022). Observability in Microservices: From Traditional Monitoring to Distributed System Intelligence. International Journal of Computer Technology and Electronics Communication, 5(6), 16220-16226.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802013

16. Anand, L. (2023). An Intelligent AI and ML–Driven Cloud Security Framework for Financial Workflows and Wastewater Analytics. International Journal of Humanities and Information Technology, 5(02), 87-94.
17. Gentyala, R. (2024). From Bronze to Broken: A Grounded Theory Study of Anti-Patterns and Accruing Data Debt in Medallion Lakehouse Deployments. European Journal of Advances in Engineering and Technology, 11(1), 90–100.
18. Kale, A., & Viswanathan, S. (2025). Global Surge in Banking Frauds: An International Management Perspective. International Journal of Accounting and Management Sciences, 4(4).
19. Appani, C., & Guda, D. P. (2023). Self-supervised representation learning for zero-day attack detection in encrypted network traffic. Computer Fraud & Security, 2023(7), 20–31. Retrieved from: https://computerfraudsecurity.com/index.php/journal/article/view/661
20. Kothokatta, L. (2025). Parallel Automation for Cross-Browser and Cross-Device Validation in OTT Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(5), 12919-12928.
21. Meka, S. (2022). Engineering Insurance Portals of the Future: Modernizing Core Systems for Performance and Scalability. International Journal of Computer Science and Information Technology Research, 3(1), 180-198.
22. Niture, N., & Abdellatif, I. (2025). A systematic review of factors, data sources, and prediction techniques for earlier prediction of traffic collision using AI and machine learning. Multimedia Tools and Applications, 84(18), 19009-19037.
23. Dama H. B. (2025). Automated database provisioning in CI/CD pipelines using Ansible and Azure DevOps. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(3), 9974–9981.
24. Viswanathan, V. (2025). Agentic AI for Employment: Reducing Unemployment through Intelligent Job-Seeker Support. LEX LOCALIS–Journal of Local Self-Government.
25. Akila, R. (2024). A deep reinforcement learning approach for optimizing inventory management in the agri-food supply chain. J. Electrical Systems, 20(4s), 2238-2247.
26. Ranjith Rajasekharan. (2018). Infrastructure as code: Transforming enterprise IT operations. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 1(1), 8–15.
27. Mangukiya, M. (2025). Advanced testing and validation frameworks for high-reliability multi-board electronic systems. International Journal of Computational and Experimental Science and Engineering, 11(4).
28. Chaturvedi, V. (2025). Disease Diagnostic Systems based on AI-Applications in Healthcare: Models, Challenges, and Future Directions. International Journal of Emerging Research in Engineering and Technology, 6(4), 207-217.
29. Gopinathan, V. R. (2024). Cyber-Resilient Digital Banking Analytics Using AI-Driven Federated Machine Learning on AWS. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8419-8426.
30. Sravanthi Mallireddy, D. R. S. (2024). Howzs Digital Transformation Impacted on HealthCare and Financial Services. Journal of Technological Innovations, 5(3).
31. Sarabhu, V. B., & Balaji, V. (2018). Advanced memory virtualization technique for efficient access of data resources in cloud environment. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 1(3), 623–629.
32. Murugeshwari, B., Amirthavalli, R., Sri, C. B., & Pari, S. N. (2023). Hybrid key authentication scheme for privacy over adhoc communication. arXiv preprint arXiv:2304.14652.
33. Anbazhagan, K. (2025). Secure AI Enabled Enterprise Ecosystems for Fraud Prevention Compliance Automation and Real Time Analytics. International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management, 1(4), 6-13.
34. Sravanthi Mallireddy, D. R. S. (2024). Howzs Digital Transformation Impacted on HealthCare and Financial Services. Journal of Technological Innovations, 5(3).
35. Yasin, M., Rahman, M. B., Kanojiya, S., & Hasan, M. (2025). Strategic decision-making in healthcare using advanced business analytics techniques. Nvpubhouse Library for International Journal of Medical Science and Public Health Research, 6(10), 163-190.
36. Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.
37. Dhinakaran, D., Prathap, P. J., Selvaraj, D., Kumar, D. A., & Murugeshwari, B. (2022). Mining privacy-preserving association rules based on parallel processing in cloud computing. International Journal of Engineering Trends and Technology, 70(3), 284-294.