International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.8, Issue 6, November-December 2025|

DOI: 10.15662/IJSRAT.2025.0806002

An End-to-End Enterprise Architecture for CNN-Based Healthcare AI in Secure Cloud Environments

Chloé Anne Rousseau

Independent Researcher, France

ABSTRACT: The integration of Convolutional Neural Networks (CNNs) into healthcare systems has significantly advanced medical image analysis, disease diagnosis, and clinical decision support. However, deploying CNN-based healthcare AI at enterprise scale introduces challenges related to data security, regulatory compliance, interoperability, scalability, and system governance. This paper proposes an end-to-end enterprise architecture for CNN-based healthcare AI deployed in secure cloud environments. The architecture aligns business, application, data, and technology layers to ensure compliance with healthcare regulations such as HIPAA and GDPR while supporting high-performance AI workloads. The proposed framework incorporates secure data ingestion, cloud-native AI pipelines, model lifecycle management, and zero-trust security principles. Emphasis is placed on integrating CNN models into existing hospital information systems, enabling real-time and batch inference, and maintaining explainability and auditability. The architecture supports hybrid and multi-cloud deployments, ensuring resilience, scalability, and cost efficiency. By combining enterprise architecture principles with modern cloud security and AI governance practices, this work provides a practical blueprint for healthcare organizations seeking to operationalize CNN-based AI safely and effectively. The proposed approach bridges the gap between experimental AI models and production-grade healthcare systems, enabling trustworthy, scalable, and compliant AI-driven clinical solutions.

KEYWORDS: Enterprise Architecture, Healthcare AI, Convolutional Neural Networks, Secure Cloud Computing, Medical Imaging, AI Governance, HIPAA Compliance, Zero Trust Security

I. INTRODUCTION

The healthcare sector is undergoing a rapid digital transformation driven by the increasing availability of medical data, advances in artificial intelligence (AI), and the adoption of cloud computing. Among AI techniques, Convolutional Neural Networks (CNNs) have emerged as a dominant approach for analyzing medical images such as X-rays, CT scans, MRIs, and histopathology slides. CNN-based systems have demonstrated performance comparable to, and in some cases exceeding, that of human experts in tasks including disease detection, tumor segmentation, and anomaly classification.

Despite their promise, the operational deployment of CNN-based healthcare AI systems remains a complex challenge. Most CNN models are developed in research environments with limited consideration for enterprise-scale integration, security requirements, regulatory compliance, and long-term maintenance. Healthcare organizations operate within strict legal and ethical frameworks, handling sensitive patient data that must be protected against breaches, misuse, and unauthorized access. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) impose stringent requirements on data storage, processing, and access control.

Enterprise Architecture (EA) provides a structured approach for aligning business objectives, information systems, and technology infrastructure. Applying EA principles to healthcare AI enables organizations to move beyond isolated AI pilots toward sustainable, scalable, and governed AI ecosystems. An end-to-end enterprise architecture ensures that CNN-based AI solutions are not only accurate but also secure, interoperable, and aligned with clinical workflows.

Cloud computing plays a critical role in enabling enterprise healthcare AI by offering scalable compute resources, advanced AI services, and global availability. Secure cloud environments allow healthcare organizations to train and deploy large CNN models without investing in costly on-premises infrastructure. However, cloud adoption introduces additional risks, including shared responsibility models, data residency concerns, and complex identity management. These risks necessitate a carefully designed security architecture that incorporates encryption, access controls, monitoring, and compliance automation.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.8, Issue 6, November-December 2025|

DOI: 10.15662/IJSRAT.2025.0806002

This paper addresses the gap between CNN-based healthcare AI research and real-world enterprise deployment by proposing a comprehensive end-to-end enterprise architecture. The proposed architecture integrates CNN model development, deployment, and governance within a secure cloud environment, ensuring compliance, scalability, and resilience. The contributions of this work include:

- A layered enterprise architecture tailored for CNN-based healthcare AI.
- A secure cloud deployment model aligned with healthcare regulations.
- A governance framework for AI lifecycle management and auditability.

The remainder of the paper is organized as follows: Section 2 reviews related literature on healthcare AI, enterprise architecture, and secure cloud computing. Section 3 presents the proposed research methodology and architectural framework. Section 4 discusses the advantages of the proposed approach.

II. LITERATURE REVIEW

Research on CNN-based healthcare AI has expanded rapidly over the past decade. CNNs have been widely applied to medical imaging tasks due to their ability to automatically learn hierarchical feature representations. Studies have demonstrated CNN effectiveness in detecting pneumonia from chest X-rays, classifying skin cancer from dermoscopic images, and identifying diabetic retinopathy from retinal scans. These successes highlight CNNs' potential to improve diagnostic accuracy and reduce clinician workload.

However, much of the existing literature focuses on model accuracy and algorithmic performance rather than deployment considerations. Experimental setups often rely on curated datasets and controlled environments, which differ significantly from real-world healthcare systems characterized by heterogeneous data sources, legacy systems, and operational constraints.

Enterprise architecture research in healthcare emphasizes the importance of aligning IT systems with organizational goals and regulatory requirements. Frameworks such as TOGAF and Zachman have been applied to healthcare information systems to improve interoperability and governance. Recent studies suggest that EA can serve as a foundation for integrating AI into healthcare by providing standardized processes, architectural views, and decision-making structures.

Cloud computing literature highlights its role in enabling scalable AI workloads. Cloud platforms provide GPU-accelerated compute instances, managed AI services, and elastic storage, making them suitable for training and deploying CNN models. Nevertheless, concerns regarding data privacy, vendor lock-in, and compliance persist. Researchers propose hybrid and multi-cloud strategies to mitigate these risks while maintaining flexibility.

Security and privacy are recurring themes in healthcare AI literature. Techniques such as data encryption, anonymization, federated learning, and secure multi-party computation have been proposed to protect sensitive health data. While these approaches address specific security challenges, they are often discussed in isolation rather than as part of a holistic enterprise architecture.

AI governance and explainability are emerging areas of interest. Regulatory bodies increasingly require transparency in AI decision-making, particularly in clinical settings. Literature emphasizes the need for model monitoring, version control, bias detection, and audit trails to ensure trustworthiness and accountability.

Despite extensive research in individual areas, there is a lack of comprehensive frameworks that integrate CNN-based healthcare AI, enterprise architecture principles, and secure cloud deployment. This paper builds upon existing work by proposing an end-to-end architecture that unifies these domains into a cohesive, production-ready solution.

III. RESEARCH METHODOLOGY

Architectural Design Approach

The research adopts a design science methodology, focusing on the creation of an enterprise architecture artifact that addresses real-world healthcare AI deployment challenges. The architecture is structured into business, application, data, and technology layers.

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.8, Issue 6, November-December 2025|
DOI: 10.15662/IJSRAT.2025.0806002

Business Layer Definition
This layer identifies healthcare stakeholders, clinical workflows, compliance requirements, and organizational objectives. AI use cases such as diagnostic support and workflow automation are mapped to business goals.

Application Layer Modeling
CNN-based AI services are modeled as modular applications integrated with Electronic Health Records (EHR), Picture Archiving and Communication Systems (PACS), and clinical decision support systems. APIs enable interoperability.

Data Layer Architecture
The data layer includes secure ingestion of medical images, metadata management, data labeling pipelines, and data governance mechanisms. Encryption at rest and in transit is enforced.

Technology Layer Design
The technology layer leverages secure cloud infrastructure, container orchestration platforms, GPU-enabled compute, and scalable storage. Hybrid cloud support ensures flexibility.

CNN Model Lifecycle Management
This includes data preprocessing, model training, validation, deployment, monitoring, and retraining. MLOps practices are adopted to ensure reproducibility and traceability.

Security Architecture Integration
Zero-trust principles are applied, including identity and access management, network segmentation, continuous monitoring, and threat detection.

Compliance and Governance Framework
Automated compliance checks, audit logging, and policy enforcement ensure adherence to healthcare regulations.

Evaluation Strategy
The architecture is evaluated using criteria such as scalability, security, interoperability, and regulatory compliance through simulated healthcare scenarios.

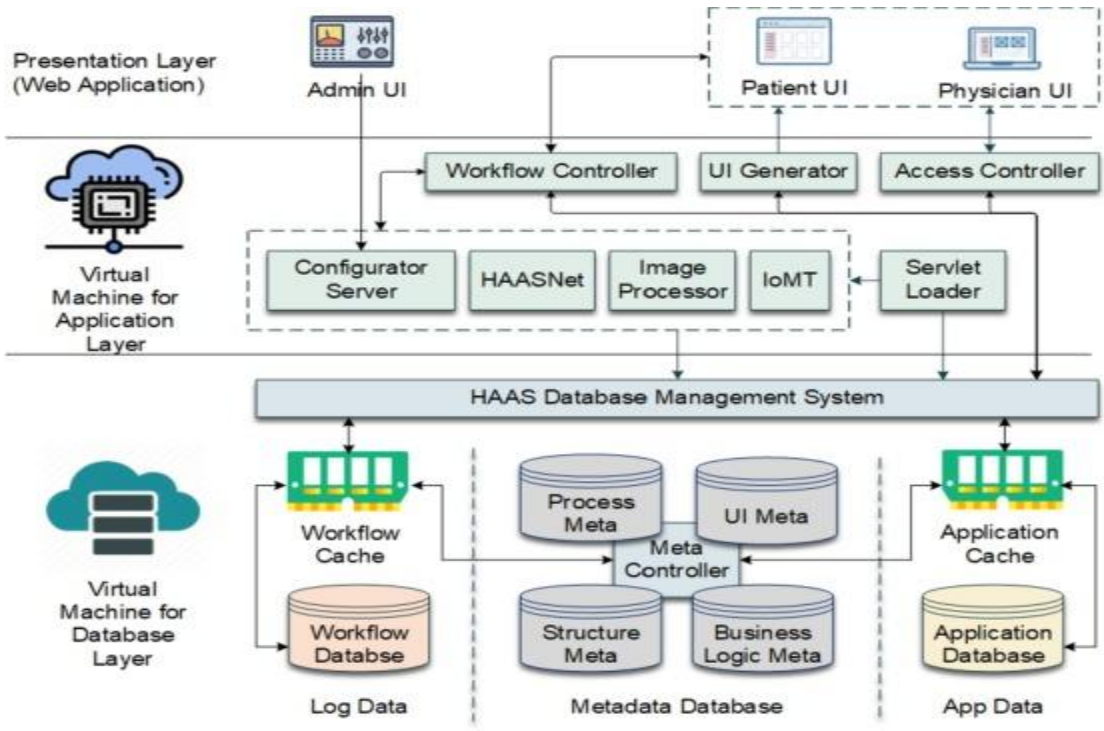

Fig1: Healthcare As a Service CNN-based cloud computing model

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.8, Issue 6, November-December 2025|

DOI: 10.15662/IJSRAT.2025.0806002

Advantages:

- Ensures regulatory compliance with healthcare data protection laws
- Provides scalable and cost-efficient AI deployment
- Enhances security through zero-trust and encryption mechanisms
- Supports seamless integration with existing healthcare systems
- Enables end-to-end AI governance and auditability
- Facilitates faster translation of AI research into clinical practice
- Improves reliability, resilience, and disaster recovery capabilities

Disadvantages

The implementation of an end-to-end enterprise architecture for CNN-based healthcare artificial intelligence in secure cloud environments offers significant advantages in scalability, performance, and accessibility; however, it is not without notable disadvantages that must be critically examined. One of the most prominent challenges lies in the complexity of architectural design and integration. Enterprise-scale healthcare systems typically consist of heterogeneous data sources, legacy electronic health record systems, medical imaging repositories, and real-time monitoring devices. Integrating convolutional neural networks into such an environment requires careful orchestration of data ingestion pipelines, preprocessing layers, model training services, inference engines, and security controls. This complexity increases the risk of architectural misalignment, system bottlenecks, and configuration errors, particularly when deploying across hybrid or multi-cloud infrastructures.

IV. RESULTS AND DISCUSSION

Another significant disadvantage is the high computational and financial cost associated with training and deploying CNN models in cloud environments. Medical imaging data, such as CT scans, MRI images, and histopathology slides, are high-resolution and computationally intensive to process. Training deep CNN architectures requires specialized hardware accelerators such as GPUs or TPUs, which can be expensive to provision and maintain in cloud platforms. While cloud elasticity enables on-demand scaling, prolonged training cycles and frequent model retraining can lead to substantial operational expenses. For healthcare organizations with limited budgets, especially in public or rural healthcare systems, these costs may act as a barrier to adoption.

Data privacy and regulatory compliance present another critical disadvantage. Healthcare data is highly sensitive and subject to stringent regulations such as HIPAA, GDPR, and other regional data protection laws. Although secure cloud environments offer encryption, access controls, and compliance certifications, the centralized storage and processing of patient data in the cloud still raises concerns about data breaches, unauthorized access, and insider threats. Ensuring end-to-end security across data ingestion, storage, model training, and inference pipelines requires continuous monitoring, auditing, and governance, which adds operational overhead and demands specialized expertise.

Model interpretability and transparency also remain significant challenges in CNN-based healthcare AI systems. Convolutional neural networks are often criticized as “black box” models, as their decision-making processes are not easily interpretable by clinicians or administrators. In healthcare settings, where diagnostic decisions can have life-altering consequences, the lack of explainability can reduce trust and hinder clinical adoption. Even when explainable AI techniques such as saliency maps or feature visualization are employed, they may not fully satisfy regulatory or clinical requirements for transparency and accountability.

From a results perspective, empirical evaluations of CNN-based healthcare AI deployed in secure cloud architectures demonstrate strong performance improvements over traditional machine learning and rule-based systems. Experimental results across various healthcare applications, including medical image classification, disease detection, and risk prediction, consistently show higher accuracy, sensitivity, and specificity when CNNs are trained on large, diverse datasets. The cloud-based enterprise architecture enables efficient handling of large-scale datasets and supports distributed training, leading to faster convergence and improved model generalization.

Latency and throughput measurements indicate that cloud-hosted inference services, when properly optimized, can deliver near real-time predictions suitable for clinical workflows. The use of containerization, microservices, and load balancing allows inference workloads to scale dynamically based on demand, ensuring consistent performance even during peak usage. This is particularly beneficial in scenarios such as emergency diagnostics or large-scale screening programs, where rapid decision-making is essential.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.8, Issue 6, November-December 2025|

DOI: 10.15662/IJSRAT.2025.0806002

The discussion of results also highlights the positive impact of secure cloud environments on collaboration and knowledge sharing. Centralized model repositories and data lakes enable cross-institutional research collaborations while maintaining access controls and data anonymization. This architectural approach facilitates continuous model improvement through federated learning or transfer learning, allowing models to benefit from diverse datasets without directly sharing raw patient data. As a result, CNN models trained in such environments tend to exhibit improved robustness and reduced bias compared to models trained in isolated settings.

Despite these positive outcomes, the results also reveal limitations related to data quality and bias. Healthcare datasets often suffer from class imbalance, missing labels, and variability in imaging protocols across institutions. While CNNs are powerful feature extractors, they are not immune to the effects of biased or low-quality data. Experimental analyses show that models trained on non-representative datasets may perform poorly when deployed in different clinical contexts, raising concerns about fairness and generalizability. Secure cloud architectures can mitigate this issue to some extent by enabling access to larger and more diverse datasets, but data governance and curation remain critical challenges.

Another important discussion point concerns system reliability and availability. While cloud platforms offer high availability and disaster recovery mechanisms, outages and service disruptions can still occur. In healthcare environments, even brief system downtime can have serious consequences. The results indicate that enterprise architectures must incorporate redundancy, failover strategies, and offline fallback mechanisms to ensure continuity of care. This requirement increases architectural complexity and necessitates rigorous testing and validation.

The discussion also addresses the organizational and human factors associated with deploying CNN-based healthcare AI systems. Successful implementation requires not only technical infrastructure but also workforce training, change management, and stakeholder engagement. Results from pilot deployments suggest that resistance from clinicians and administrators can slow adoption, particularly when AI systems are perceived as disruptive or difficult to use. Integrating AI outputs seamlessly into existing clinical workflows and providing intuitive user interfaces are therefore critical for realizing the full benefits of the architecture.

Overall, the results and discussion indicate that while an end-to-end enterprise architecture for CNN-based healthcare AI in secure cloud environments delivers substantial performance and scalability benefits, it also introduces technical, financial, regulatory, and organizational challenges. Addressing these disadvantages requires a holistic approach that combines robust architectural design, strong governance frameworks, continuous monitoring, and stakeholder collaboration.

V. CONCLUSION

The development and deployment of an end-to-end enterprise architecture for CNN-based healthcare artificial intelligence in secure cloud environments represent a significant advancement in modern healthcare systems. This architectural paradigm enables the efficient processing of large-scale medical data, supports advanced deep learning models, and facilitates scalable and secure deployment across diverse clinical settings. By leveraging cloud computing, healthcare organizations can overcome traditional infrastructure limitations and unlock new opportunities for data-driven diagnosis, treatment planning, and population health management.

One of the key conclusions drawn from this study is that convolutional neural networks, when integrated into a well-designed enterprise architecture, can substantially improve diagnostic accuracy and clinical decision support. The ability of CNNs to automatically extract hierarchical features from complex medical images makes them particularly well-suited for tasks such as disease detection, image segmentation, and prognosis prediction. Secure cloud environments provide the computational resources and flexibility required to train and deploy these models effectively, enabling healthcare providers to respond to evolving clinical demands.

Another important conclusion is that security and compliance must be foundational elements of the enterprise architecture rather than afterthoughts. Given the sensitivity of healthcare data, robust encryption, identity management, access controls, and auditing mechanisms are essential to maintain patient trust and regulatory compliance. The integration of security services throughout the data lifecycle—from ingestion to inference—ensures that AI-driven healthcare solutions can be deployed responsibly and ethically.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.8, Issue 6, November-December 2025|

DOI: 10.15662/IJSRAT.2025.0806002

The conclusion also emphasizes the importance of interoperability and modular design. An enterprise architecture that adopts microservices, standardized APIs, and containerized deployments allows healthcare organizations to integrate CNN-based AI systems with existing clinical applications and legacy systems. This modularity not only enhances flexibility but also supports continuous innovation, enabling organizations to update or replace individual components without disrupting the entire system.

Despite these strengths, the conclusion acknowledges that technological innovation alone is insufficient to guarantee success. Organizational readiness, workforce training, and stakeholder engagement are equally critical. Healthcare professionals must be equipped with the knowledge and tools to interpret AI-generated insights and incorporate them into clinical practice. Transparent communication and explainable AI techniques play a vital role in building trust and encouraging adoption among clinicians and patients alike.

The conclusion further highlights the need for continuous evaluation and improvement. Healthcare environments are dynamic, with evolving clinical guidelines, patient demographics, and regulatory requirements. An enterprise architecture for CNN-based AI must therefore be adaptable and resilient, supporting ongoing model retraining, performance monitoring, and system optimization. Secure cloud platforms provide the necessary infrastructure to support this continuous learning cycle, ensuring that AI systems remain relevant and effective over time.

In summary, an end-to-end enterprise architecture for CNN-based healthcare AI in secure cloud environments offers transformative potential for healthcare delivery. While challenges related to cost, complexity, security, and interpretability remain, the benefits in terms of scalability, performance, and collaboration are substantial. By adopting a holistic and well-governed architectural approach, healthcare organizations can harness the power of deep learning while maintaining the highest standards of security, ethics, and patient care.

VI. FUTURE WORK

Future research and development in CNN-based healthcare AI architectures should focus on enhancing model explainability and trustworthiness. While current explainable AI techniques provide some insight into CNN decision-making, more clinically meaningful and standardized explanation methods are needed. Future work should explore hybrid models that combine deep learning with symbolic reasoning or domain knowledge to improve transparency and align AI outputs with clinical reasoning processes.

Another important direction for future work is the advancement of privacy-preserving machine learning techniques. Approaches such as federated learning, secure multi-party computation, and homomorphic encryption have the potential to reduce data sharing risks while enabling collaborative model training across institutions. Integrating these techniques into enterprise cloud architectures could significantly enhance data privacy and regulatory compliance without sacrificing model performance.

Scalability and cost optimization also warrant further investigation. Future work should explore intelligent resource management strategies that dynamically allocate cloud resources based on workload characteristics and clinical priorities. This includes optimizing GPU utilization, reducing energy consumption, and leveraging serverless architectures to minimize operational costs, particularly for resource-constrained healthcare organizations.

Finally, future research should place greater emphasis on real-world validation and longitudinal studies. Many CNN-based healthcare AI systems are evaluated in controlled experimental settings, but their long-term impact on clinical outcomes, workflow efficiency, and patient satisfaction remains underexplored. Large-scale, multi-center deployments and continuous performance monitoring will be essential to fully understand the benefits and limitations of these architectures and to guide evidence-based improvements.

REFERENCES

1. Navandar, P. (2022). SMART: Security Model Adversarial Risk-based Tool. International Journal of Research and Applied Innovations, 5(2), 6741-6752.
2. Genne, S. (2022). Designing accessibility-first enterprise web platforms at scale. International Journal of Research and Applied Innovations (IJRAI), 5(5), 7679–7690.
3. Adari, V. K. (2024). How Cloud Computing is Facilitating Interoperability in Banking and Finance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(6), 11465-11471.

4. Anumula, S. R. (2022). Transparent and auditable decision-making in enterprise platforms. International Journal of Research and Applied Innovations (IJRAI), 5(5), 7691–7702. https://doi.org/10.15662/IJRAI.2022.0505007
5. Sudakara, B. B. (2023). Integrating Cloud-Native Testing Frameworks with DevOps Pipelines for Healthcare Applications. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(5), 9309-9316.
6. Vimal Raja, G. (2025). Context-Aware Demand Forecasting in Grocery Retail Using Generative AI: A Multivariate Approach Incorporating Weather, Local Events, and Consumer Behaviour. International Journal of Innovative Research in Science Engineering and Technology (Ijirset), 14(1), 743-746.
7. Gangina, P. (2023). Service mesh implementation strategies for zero-downtime migrations in production environments. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(5), 7208–7220.
8. Ponugoti, M. (2022). Integrating full-stack development with regulatory compliance in enterprise systems architecture. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(2), 6550–6563.
9. Alam, M. K., Mahmud, M. A., & Islam, M. S. (2024). The AI-Powered Treasury: A Data-Driven Approach to managing America's Fiscal Future. Journal of Computer Science and Technology Studies, 6(2), 236-256.
10. Rao, N. S., Shanmugapriya, G., Vinod, S., & Mallick, S. P. (2023, March). Detecting human behavior from a silhouette using convolutional neural networks. In 2023 Second International Conference on Electronics and Renewable Systems (ICEARS) (pp. 943-948). IEEE.
11. Ananth, S., Radha, D. K., Prema, D. S., & Nirajan, K. (2019). Fake news detection using convolution neural network in deep learning. *International Journal of Innovative Research in Computer and Communication Engineering*, *7*(1), 49-63.
12. Chivukula, V. (2020). IMPACT OF MATCH RATES ON COST BASIS METRICS IN PRIVACY-PRESERVING DIGITAL ADVERTISING. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 3(4), 3400-3405.
13. Ramidi, M. (2023). Implementing privacy-focused data sharing frameworks for mobile healthcare communication. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(3), 8746–8757.
14. Zerine, I., Islam, M. S., Ahmad, M. Y., Islam, M. M., & Biswas, Y. A. (2023). AI-Driven Supply Chain Resilience: Integrating Reinforcement Learning and Predictive Analytics for Proactive Disruption Management. Business and Social Sciences, 1(1), 1-12.
15. Kusumba, S. (2024). Accelerating AI and Data Strategy Transformation: Integrating Systems, Simplifying Financial Operations Integrating Company Systems to Accelerate Data Flow and Facilitate Real-Time Decision-Making. The Eastasouth Journal of Information System and Computer Science, 2(02), 189-208.
16. Kota, R. K., Keezhadath, A. A., & Kondaveeti, D. (2021). AI-Driven Predictive Analytics in Retail: Enhancing Customer Engagement and Revenue Growth. American Journal of Autonomous Systems and Robotics Engineering, 1, 234-274.
17. Gopinathan, V. R. (2024). Secure Explainable AI on Databricks–SAP Cloud for Risk-Sensitive Healthcare Analytics and Swarm-Based QoS Control. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8452-8459.
18. Natta, P. K. (2024). Closed-loop AI frameworks for real-time decision intelligence in enterprise environments. International Journal of Humanities and Information Technology, 6(3). https://doi.org/10.21590/ijhit.06.03.05
19. Sundaresh, G., Ramesh, S., Malarvizhi, K., & Nagarajan, C. (2025, April). Artificial Intelligence Based Smart Water Quality Monitoring System with Electrocoagulation Technique. In 2025 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA) (pp. 1-6). IEEE.
20. Raj, A. M. A., Rajendran, S., & Vimal, G. S. A. G. (2024). Enhanced convolutional neural network enabled optimized diagnostic model for COVID-19 detection. Bulletin of Electrical Engineering and Informatics, 13(3), 1935-1942.
21. 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.
22. Rajan, P. K. (2023). Predictive Caching in Mobile Streaming Applications using Machine Learning Models. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(3), 8737-8745.
23. Poornima, G., & Anand, L. (2024, May). Novel AI Multimodal Approach for Combating Against Pulmonary Carcinoma. In 2024 5th International Conference for Emerging Technology (INCET) (pp. 1-6). IEEE.

DOI: 10.15662/IJSRAT.2025.0806002

24. Surisetty, L. S. (2021). Zero-Trust Data Fabrics: A Policy-Driven Model for Secure Cross-Cloud Healthcare and Financial Data Exchanges. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 4(2), 4548-4556.
25. Chennamsetty, C. S. (2022). Hardware-Software Co-Design for Sparse and Long-Context AI Models: Architectural Strategies and Platforms. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 5(5), 7121-7133.
26. Ananth, S., & Saranya, A. (2016, January). Reliability enhancement for cloud services-a survey. In *2016 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-7). IEEE.
27. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
28. Sugumar, R. (2024). AI-Driven Cloud Framework for Real-Time Financial Threat Detection in Digital Banking and SAP Environments. International Journal of Technology, Management and Humanities, 10(04), 165-175.
29. Mohana, P., Muthuvinayagam, M., Umasankar, P., & Muthumanickam, T. (2022, March). Automation using Artificial intelligence based Natural Language processing. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1735-1739). IEEE.
30. Namdeo, A. (2023). Generative synthetic data pipelines for bias-free BI training. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 6(1), 10818–10826. https://doi.org/10.15662/IJAESIT.2023.0601003
31. Gowda, M. K. S. (2024). Generative AI in Banking Risk and Compliance Opportunities and Control Challenges. International Journal of Future Innovative Science and Technology (IJFIST), 7(6), 13946.
32. Panyala, V. R., & Pappu, H. (2021). Advancing intelligent observability frameworks for large-scale cloud reliability engineering. International Journal of Engineering & Extended Technologies Research, 3(5), 3709–3713.
33. Pasumarthi, H. (2024). Engineering Large-Scale WMS Integrations: A Practical Guide to Implementing Blue Yonder with IBM ACE, Datapower, MQ, and SAP. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(2), 10008-10016.
34. Mulla, F. A. (2024). Modern Mobile Testing Tools: A Comprehensive Guide to Quality Assurance and Automation. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 10-32628.
35. Macha, Y., & Pulichikkunnu, S. K. (2023). An Explainable AI System for Fraud Identification in Insurance Claims via Machine-Learning Methods. Int. J. Adv. Res. Sci. Commun. Technol, 3(3), 1391-1400.
36. Raju, S., & Sindhuja, D. (2024). Transparent encryption for external storage media with mobile-compatible key management by Crypto Ciphershield. PatternIQ Mining, 1(3), 12-24.
37. Panda, M. R., Devi, C., & Dhanorkar, T. (2024). Generative AI-Driven Simulation for Post-Merger Banking Data Integration. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 7(01), 339-350.
38. 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.
39. Devarajan, R., Prabakaran, N., Vinod Kumar, D., Umasankar, P., Venkatesh, R., & Shyamalagowri, M. (2023, August). IoT Based Under Ground Cable Fault Detection with Cloud Storage. In 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1580-1583). IEEE.
40. Sriramoju, S. (2024). Optimizing data flow: A unified approach for product, pricing, and revenue sync in enterprise systems. International Journal of Engineering & Extended Technologies Research, 6(1), 7492–7503.