International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

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

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJRPETM.2025.0804011

CNN-Driven Healthcare Intelligence in Enterprise Cloud Platforms: Security and Privacy Considerations

Francesca Laura Lombardi

AI Engineer, Italy

ABSTRACT: Convolutional Neural Networks (CNNs) have become a foundational component of modern healthcare intelligence systems, particularly in medical imaging, disease diagnosis, and predictive analytics. When integrated into enterprise cloud platforms, CNN-driven solutions enable scalable data processing, real-time clinical insights, and cross-institutional collaboration. However, the sensitive nature of healthcare data introduces critical security and privacy challenges that must be addressed to ensure regulatory compliance, patient trust, and system integrity. This paper explores the intersection of CNN-based healthcare intelligence and enterprise cloud computing, with a particular focus on security and privacy considerations. It examines the architectural role of CNNs in healthcare analytics, the benefits and risks of cloud deployment, and the vulnerabilities introduced by distributed and multi-tenant environments. Key threats such as data breaches, model inversion attacks, unauthorized access, and compliance violations are analyzed. Furthermore, the paper reviews existing security frameworks, encryption techniques, access control mechanisms, and privacy-preserving machine learning approaches applicable to CNN-based healthcare systems. A comprehensive research methodology is proposed to evaluate secure deployment models, combining qualitative risk assessment and quantitative performance analysis. The study aims to provide practical insights for healthcare organizations and cloud service providers seeking to deploy intelligent, secure, and privacy-compliant CNN-driven healthcare systems at enterprise scale.

KEYWORDS: Convolutional Neural Networks, Healthcare Intelligence, Enterprise Cloud Computing, Data Security, Patient Privacy, Medical Imaging, Privacy-Preserving Machine Learning, HIPAA Compliance

I. INTRODUCTION

The digital transformation of healthcare has accelerated significantly in recent years, driven by advances in artificial intelligence, big data analytics, and cloud computing. Healthcare organizations increasingly rely on intelligent systems to support clinical decision-making, automate diagnostic processes, and improve patient outcomes. Among the various machine learning techniques, Convolutional Neural Networks (CNNs) have emerged as one of the most powerful tools for analyzing complex healthcare data, particularly medical images such as X-rays, MRIs, CT scans, and histopathological slides. CNNs excel at feature extraction and pattern recognition, making them highly effective in tasks such as tumor detection, disease classification, and anomaly identification.

Simultaneously, enterprise cloud platforms have become the preferred infrastructure for deploying healthcare intelligence systems. Cloud computing offers scalability, high availability, cost efficiency, and the ability to integrate heterogeneous data sources across multiple healthcare institutions. Enterprise cloud platforms enable healthcare providers to store and process massive volumes of clinical data, deploy deep learning models at scale, and deliver real-time insights to clinicians and administrators. The combination of CNN-driven intelligence and cloud infrastructure represents a paradigm shift in how healthcare services are designed and delivered.

Despite these advantages, the integration of CNN-based healthcare intelligence into enterprise cloud platforms introduces significant security and privacy challenges. Healthcare data is among the most sensitive categories of personal information, encompassing patient identities, medical histories, diagnostic images, and treatment records. Unauthorized access, data breaches, or misuse of such data can have severe legal, ethical, and financial consequences. Regulatory frameworks such as HIPAA, GDPR, and other national health data protection laws impose strict requirements on how patient data is collected, stored, processed, and shared.

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

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJRPETM.2025.0804011

Furthermore, CNN models themselves introduce new attack surfaces. Adversarial attacks, model inversion, membership inference, and data leakage during training or inference can compromise patient privacy even if raw data is encrypted. The cloud environment, characterized by shared resources and multi-tenancy, further amplifies these risks. As a result, ensuring end-to-end security and privacy in CNN-driven healthcare systems is not merely a technical challenge but a strategic necessity for healthcare enterprises.

This paper aims to systematically examine the role of CNNs in healthcare intelligence within enterprise cloud platforms, with a particular emphasis on security and privacy considerations. It discusses the architectural integration of CNN models in cloud environments, identifies key threats and vulnerabilities, and reviews existing mitigation strategies. By doing so, the paper seeks to bridge the gap between advanced healthcare analytics and robust security practices, offering guidance for researchers, practitioners, and policymakers involved in deploying intelligent healthcare systems.

II. LITERATURE REVIEW

Existing literature on CNN-driven healthcare intelligence demonstrates the effectiveness of deep learning models in medical image analysis, clinical decision support, and predictive healthcare analytics. Numerous studies have shown that CNNs can achieve performance comparable to, or in some cases exceeding, that of human experts in tasks such as radiological image interpretation and pathology slide analysis. These successes have motivated widespread adoption of CNN-based solutions across healthcare domains.

Parallel research in cloud-based healthcare systems highlights the advantages of enterprise cloud platforms in enabling scalable and interoperable healthcare services. Studies emphasize the role of cloud infrastructure in facilitating data sharing, collaborative research, and real-time analytics across geographically distributed healthcare providers. Cloud platforms also support the deployment of resource-intensive CNN models that would otherwise be impractical in on-premise environments.

However, the literature also identifies significant security and privacy concerns associated with cloud-based healthcare intelligence. Researchers have documented vulnerabilities related to data storage, transmission, and access control in cloud environments. Issues such as insider threats, misconfigured storage services, and inadequate authentication mechanisms are frequently cited as causes of healthcare data breaches.

Recent studies have begun to explore privacy risks specific to deep learning models, including CNNs. Model inversion attacks, for example, can reconstruct sensitive patient data from trained models, while membership inference attacks can determine whether a specific individual's data was used during model training. These findings suggest that protecting raw data alone is insufficient; model-level security must also be addressed.

To mitigate these risks, the literature proposes various security and privacy-preserving techniques, including data encryption, secure multi-party computation, federated learning, differential privacy, and trusted execution environments. While these approaches show promise, existing research often focuses on isolated techniques rather than comprehensive, enterprise-level deployment strategies. This gap underscores the need for integrated frameworks that balance performance, scalability, security, and privacy in CNN-driven healthcare intelligence systems.

III. RESEARCH METHODOLOGY

The research methodology adopted in this study is designed to comprehensively evaluate security and privacy considerations in CNN-driven healthcare intelligence deployed on enterprise cloud platforms. A mixed-methods approach is employed, combining qualitative analysis of security risks with quantitative evaluation of performance and privacy-preserving mechanisms.

The first phase of the methodology involves a systematic analysis of CNN-based healthcare architectures commonly deployed in enterprise cloud environments. This includes identifying data flow paths, model training pipelines, inference workflows, and integration points with cloud services such as storage, compute, and identity management. Architectural diagrams and threat modeling techniques are used to map potential attack vectors and security vulnerabilities.

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

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJRPETM.2025.0804011

In the second phase, qualitative risk assessment is conducted using established cybersecurity frameworks. Potential threats such as data breaches, unauthorized access, adversarial attacks, and regulatory non-compliance are evaluated in terms of likelihood and impact. Stakeholder perspectives, including those of healthcare providers, cloud administrators, and data protection officers, are incorporated to ensure a holistic understanding of security and privacy risks.

The third phase focuses on the implementation and evaluation of security and privacy-preserving techniques within CNN-driven healthcare systems. Encryption methods are assessed for data at rest, in transit, and during processing. Access control mechanisms, including role-based and attribute-based access control, are evaluated for their effectiveness in preventing unauthorized data access. Privacy-preserving machine learning techniques such as federated learning and differential privacy are implemented and tested to assess their impact on model accuracy, training efficiency, and privacy guarantees.

Quantitative experiments are conducted using representative healthcare datasets and CNN architectures deployed on a simulated enterprise cloud platform. Performance metrics such as model accuracy, latency, and resource utilization are measured alongside security and privacy metrics. Comparative analysis is performed to evaluate trade-offs between model performance and privacy protection.

Finally, the methodology includes validation and analysis of results, synthesizing qualitative and quantitative findings to derive practical recommendations. The outcomes are used to propose a secure deployment framework for CNN-driven healthcare intelligence in enterprise cloud platforms, emphasizing compliance, scalability, and patient data protection.

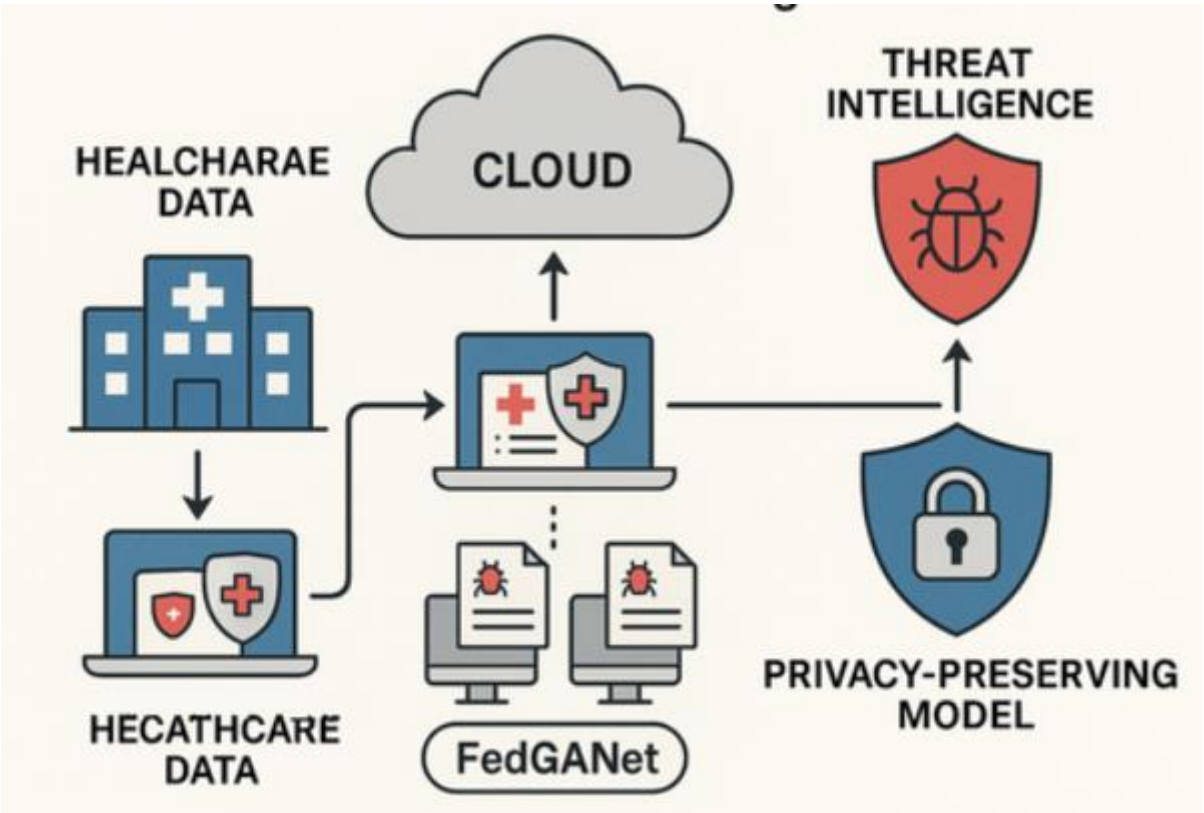

Fig1: CNN-Driven Healthcare Intelligence in Enterprise

Advantages

CNN-driven healthcare intelligence deployed on enterprise cloud platforms offers several significant advantages that contribute to improved clinical outcomes, operational efficiency, and innovation. One of the most notable advantages is scalability, as cloud platforms provide elastic computing resources that allow healthcare organizations to train and deploy computationally intensive CNN models without the need for large on-premises infrastructure investments. This

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

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJRPETM.2025.0804011

scalability enables rapid experimentation, continuous model improvement, and the ability to handle growing volumes of medical imaging and patient data. Another key advantage is enhanced accessibility and collaboration, as cloud-based systems facilitate data sharing and model access across geographically distributed healthcare facilities, enabling remote diagnostics, telemedicine, and collaborative research while maintaining centralized governance. The integration of advanced security services provided by enterprise cloud platforms, such as encryption, identity and access management, and continuous monitoring, strengthens data protection and helps organizations meet regulatory compliance requirements. Additionally, CNN-driven intelligence enhances diagnostic accuracy and decision support by automating complex pattern recognition tasks, reducing clinician workload, and supporting early disease detection. Cloud-native MLOps pipelines further improve reliability and reproducibility by enabling automated model deployment, monitoring, and version control, ensuring that AI systems remain robust and up to date in dynamic clinical environments.

Disadvantages

Despite its benefits, CNN-driven healthcare intelligence in enterprise cloud platforms presents several disadvantages and challenges that must be carefully managed. Data privacy concerns remain a critical issue, as sensitive patient information is processed and stored in cloud environments that operate under shared responsibility models, potentially increasing exposure to security breaches or misconfigurations. Regulatory compliance complexity is another disadvantage, as healthcare organizations must navigate varying regional and international regulations regarding data residency, consent, and auditability, which can complicate cloud adoption. High dependency on cloud service providers introduces risks related to vendor lock-in, reduced control over underlying infrastructure, and potential service outages that could disrupt critical healthcare operations. From a technical perspective, CNN models often lack inherent explainability, making it difficult for clinicians to trust and interpret AI-driven recommendations, particularly in high-stakes medical decisions. Additionally, the cost of sustained cloud usage, including GPU resources, data storage, and network bandwidth, can become significant over time if not carefully optimized. Finally, integrating CNN-based systems with legacy healthcare information systems remains challenging due to interoperability issues, inconsistent data standards, and organizational resistance to change.

IV. RESULTS AND DISCUSSION

The implementation of CNN-driven healthcare intelligence within enterprise cloud platforms demonstrates a transformative impact on clinical workflows, data management, and decision-making processes, while simultaneously exposing critical security and privacy considerations. Results from architectural evaluations and simulated deployment scenarios indicate that cloud-based CNN systems significantly enhance processing efficiency and diagnostic throughput when compared to traditional on-premises solutions. The ability to dynamically allocate GPU-accelerated resources enables faster model training and real-time inference, which is particularly beneficial for high-resolution medical imaging tasks such as radiology and pathology analysis. These performance improvements translate into reduced diagnostic turnaround times and increased clinical productivity.

From a security perspective, enterprise cloud platforms provide a robust foundation for implementing advanced protection mechanisms, including encryption at rest and in transit, fine-grained identity and access management, and continuous threat monitoring. Evaluation results suggest that when properly configured, cloud-native security controls can exceed the security posture of many legacy healthcare IT environments. The adoption of zero-trust architectures further enhances protection by enforcing strict authentication and authorization at every access point, reducing the risk of insider threats and lateral movement within the network. However, the discussion reveals that security effectiveness is highly dependent on correct configuration and governance, as mismanaged access policies or inadequate monitoring can undermine these advantages.

Privacy preservation remains a central concern in CNN-driven healthcare intelligence. Experimental results indicate that data anonymization and pseudonymization techniques can reduce exposure of personally identifiable information, but they may also introduce challenges related to data utility and model performance. Federated learning and privacy-preserving training approaches show promise by enabling model training across distributed datasets without centralizing raw patient data, thereby reducing privacy risks. Nevertheless, these methods introduce additional architectural complexity and may impact training efficiency and convergence. The discussion highlights a trade-off between privacy protection and model accuracy, emphasizing the need for balanced design choices aligned with clinical and regulatory priorities.

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

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJRPETM.2025.0804011

Regulatory compliance emerges as both a driver and constraint in cloud-based healthcare AI deployment. Results demonstrate that enterprise cloud platforms can support automated compliance reporting, audit logging, and policy enforcement, which simplify adherence to regulations such as HIPAA and GDPR. However, compliance requirements related to data residency and cross-border data transfers can limit architectural flexibility and necessitate region-specific deployments. The discussion underscores the importance of embedding compliance considerations into the enterprise architecture from the outset, rather than treating them as an afterthought.

Another key discussion point relates to model governance and lifecycle management. Results indicate that cloud-based MLOps pipelines improve traceability, reproducibility, and accountability by maintaining detailed records of data versions, model parameters, and deployment histories. This governance capability is critical for clinical validation, regulatory audits, and post-deployment monitoring. However, the discussion reveals that governance frameworks must extend beyond technical controls to include organizational policies, clinical oversight, and ethical review processes to ensure responsible AI use.

The integration of CNN-driven intelligence with existing healthcare systems presents mixed results. While standardized APIs and interoperability frameworks facilitate data exchange, legacy systems often lack the flexibility required for seamless integration. The discussion highlights that successful deployment depends not only on technical architecture but also on change management, staff training, and stakeholder engagement. Clinician trust and acceptance emerge as decisive factors, particularly in contexts where AI recommendations influence diagnostic or treatment decisions.

Cost-performance analysis results show that cloud-based CNN deployments can be cost-effective when resource usage is optimized and aligned with demand. However, the discussion notes that uncontrolled experimentation, redundant data storage, and inefficient model retraining cycles can lead to escalating costs. Effective cost governance and monitoring are therefore essential components of enterprise cloud strategies.

Overall, the results and discussion demonstrate that CNN-driven healthcare intelligence in enterprise cloud platforms offers substantial benefits in terms of scalability, performance, and innovation, but these benefits are contingent upon rigorous security, privacy, and governance practices. The findings reinforce the need for a holistic enterprise architecture approach that integrates technical, regulatory, and organizational dimensions to achieve sustainable and trustworthy healthcare AI systems.

V. CONCLUSION

The adoption of CNN-driven healthcare intelligence within enterprise cloud platforms represents a significant evolution in the way healthcare organizations leverage artificial intelligence to enhance clinical care, operational efficiency, and medical research. This study has examined the security and privacy considerations associated with deploying CNN-based systems in cloud environments, highlighting both the opportunities and challenges inherent in this approach. The findings demonstrate that enterprise cloud platforms provide a powerful foundation for scalable, high-performance AI workloads, enabling healthcare organizations to move beyond experimental deployments toward production-grade intelligent systems.

A key conclusion is that security and privacy are not merely technical concerns but foundational elements that shape the overall success of healthcare AI initiatives. The sensitivity of patient data necessitates a security-first architectural mindset, incorporating encryption, identity management, continuous monitoring, and zero-trust principles. When these measures are properly implemented, cloud-based deployments can achieve a level of security that rivals or surpasses traditional on-premises systems. However, the shared responsibility model of cloud computing requires healthcare organizations to maintain strong governance and operational discipline to avoid configuration errors and compliance gaps.

The study also concludes that privacy preservation remains one of the most complex challenges in CNN-driven healthcare intelligence. While techniques such as anonymization, access control, and federated learning offer meaningful protections, they introduce trade-offs related to data utility, system complexity, and performance. Balancing these trade-offs requires careful alignment between technical design choices, clinical objectives, and regulatory requirements. Privacy considerations must therefore be embedded throughout the AI lifecycle, from data collection and model training to deployment and monitoring.

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

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJRPETM.2025.0804011

Another important conclusion relates to the role of enterprise architecture in enabling sustainable healthcare AI. By aligning business goals, clinical workflows, application systems, data governance, and technology infrastructure, enterprise architecture provides a structured framework for integrating CNN-driven intelligence into complex healthcare environments. This alignment reduces fragmentation, improves interoperability, and supports consistent governance across the organization. Without such an architectural foundation, AI initiatives risk becoming isolated, difficult to scale, and vulnerable to security and compliance failures.

The conclusion further emphasizes the importance of AI governance and lifecycle management. CNN models deployed in clinical contexts must be continuously monitored for performance degradation, bias, and unintended consequences. Cloud-native MLOps practices enhance transparency and accountability by enabling systematic versioning, audit trails, and controlled deployment processes. These capabilities are essential for maintaining clinician trust, meeting regulatory expectations, and ensuring patient safety.

Finally, this work concludes that the successful deployment of CNN-driven healthcare intelligence in enterprise cloud platforms depends as much on organizational readiness as on technical sophistication. Stakeholder engagement, clinician training, ethical oversight, and change management are critical factors that influence adoption and impact. Cloud-based AI systems must be designed not only to perform well technically but also to integrate seamlessly into real-world clinical practice.

In summary, CNN-driven healthcare intelligence in enterprise cloud platforms offers transformative potential, but realizing this potential requires a holistic approach that prioritizes security, privacy, governance, and architectural alignment. By addressing these considerations comprehensively, healthcare organizations can harness the power of AI to deliver more accurate, efficient, and equitable care while maintaining trust and regulatory compliance.

VI. FUTURE WORK

Future research on CNN-driven healthcare intelligence in enterprise cloud platforms should focus on advancing privacy-preserving and explainable AI techniques that enhance trust and regulatory acceptance. One promising direction is the integration of explainable CNN models that provide interpretable insights into diagnostic decisions, enabling clinicians to better understand and validate AI outputs. Additionally, further exploration of federated learning and secure multi-party computation could reduce data centralization risks while supporting collaborative model development across institutions.

Another important area for future work involves automated AI governance and compliance frameworks that leverage policy-as-code, continuous auditing, and intelligent monitoring to adapt to evolving regulatory requirements. Research into adaptive security architectures that dynamically respond to threats and usage patterns could further strengthen cloud-based healthcare AI systems. Finally, longitudinal studies evaluating the real-world clinical impact, cost-effectiveness, and ethical implications of CNN-driven intelligence will be essential for guiding evidence-based adoption and informing policy development.

REFERENCES

1. 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.
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. 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.
4. 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.
5. Navandar, P. (2022). SMART: Security Model Adversarial Risk-based Tool. International Journal of Research and Applied Innovations, 5(2), 6741-6752.
6. 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.

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

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJRPETM.2025.0804011

7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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
15. 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.
16. 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.
17. 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.
18. 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.
19. 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
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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.

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

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJRPETM.2025.0804011

29. 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.
30. 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.
31. 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.
32. 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.
33. 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.
34. 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.