International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com || A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806027

Cross-Domain Cloud Architecture with AI Integration for Public Biomedical Systems and Secure Enterprise Automation

Dr. Abhishek Pratap Singh

Assistant Professor, ADYPSOCE, Pune, India

ABSTRACT: Public sector biomedical systems increasingly rely on cloud computing and AI technologies to process, analyze, and manage large-scale health data, while enterprise automation requires integration across heterogeneous systems. This paper proposes a cross-domain, AI-driven cloud architecture designed to support biomedical data processing, enterprise automation, and secure, equitable digital access. The architecture leverages AI for predictive analytics, process optimization, anomaly detection, and decision support. Cloud infrastructure enables scalability, fault tolerance, and efficient resource utilization, while microservices and containerization facilitate modularity and interoperability. The framework incorporates advanced security mechanisms, including role-based access control, encryption, and identity management, ensuring compliance with privacy regulations and equitable access to services across socio-economic and geographic demographics. The study evaluates the architecture in terms of performance, reliability, security, and accessibility. It highlights challenges such as heterogeneous data integration, interoperability, AI model bias, and regulatory compliance. Advantages include improved operational efficiency, data-driven decision-making, and enhanced accessibility. Disadvantages involve computational complexity, potential AI bias, and resource-intensive infrastructure. The proposed AI-driven cross-domain cloud architecture provides a blueprint for integrating public sector biomedical systems with enterprise automation, offering secure, scalable, and equitable digital services for diverse populations.

KEYWORDS: AI-driven cloud architecture, cross-domain systems, biomedical systems, enterprise automation, secure digital access, equitable technology, public sector IT, cloud computing.

I. INTRODUCTION

The integration of artificial intelligence (AI) and cloud computing has transformed the landscape of public sector services, particularly in biomedical systems and enterprise automation. Biomedical systems, including electronic health records (EHR), laboratory management, and epidemiological surveillance, generate vast volumes of sensitive data requiring real-time processing, advanced analytics, and secure storage. Similarly, enterprise automation in the public sector—including workflow optimization, resource management, and administrative functions—demands scalable infrastructure, data interoperability, and process automation. The convergence of AI and cloud-based solutions offers opportunities to address these challenges, facilitating predictive analytics, decision support, and intelligent resource allocation across multiple domains.

Cross-domain systems architecture refers to frameworks that integrate heterogeneous systems across different functional areas while maintaining interoperability, security, and scalability. In the context of public sector biomedical and enterprise systems, such architectures must accommodate diverse data types (structured, unstructured, and semi-structured), varying security policies, regulatory constraints, and user access requirements. The architecture must also ensure equitable digital access, particularly for underserved populations, by supporting low-bandwidth deployments, secure authentication, and inclusive service design.

AI-driven cloud architectures enable intelligent automation across multiple domains. In biomedical systems, AI algorithms—including deep learning, natural language processing, and predictive modeling—support disease diagnosis, patient monitoring, resource forecasting, and anomaly detection. In enterprise automation, AI optimizes workflows, automates repetitive tasks, detects inefficiencies, and provides decision support for policy implementation. When deployed on cloud infrastructure, these AI capabilities scale elastically, allowing real-time processing of large datasets while minimizing infrastructure costs and operational overhead.

| ISSN: 2320-0081 | www.ijctece.com || A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806027

Key design principles for cross-domain AI-driven cloud architectures include modularity, interoperability, security, and equitable access. Modularity is achieved through microservices and containerized applications, enabling independent deployment, scaling, and maintenance of individual components. Interoperability relies on standardized data exchange protocols, APIs, and integration middleware to allow seamless communication between biomedical, enterprise, and external systems. Security encompasses encryption of data at rest and in transit, identity and access management, anomaly detection, and compliance with regulations such as HIPAA and GDPR. Equitable digital access emphasizes inclusive system design, user-friendly interfaces, accessibility features, and policies that prioritize underserved populations.

The architecture addresses key challenges in public sector biomedical systems. First, it mitigates data silos by enabling cross-domain data integration, linking clinical, laboratory, and administrative datasets. Second, it supports predictive modeling for public health decision-making, including outbreak prediction, resource allocation, and personalized patient care. Third, it improves operational efficiency in enterprise automation, reducing manual interventions, and streamlining administrative workflows. The combination of AI and cloud computing allows continuous learning from data, enhancing system intelligence and adaptability.

However, deploying cross-domain AI-driven cloud architectures presents significant challenges. Data heterogeneity complicates integration across biomedical and enterprise systems, requiring advanced ETL pipelines, data normalization, and semantic mapping. AI model bias poses ethical concerns, particularly in healthcare, where biased predictions can affect patient outcomes. Regulatory compliance adds complexity, as biomedical data is highly sensitive, and public sector systems must adhere to strict legal frameworks. Additionally, cloud deployment involves resource-intensive infrastructure, latency considerations, and potential reliance on third-party cloud providers, raising concerns about vendor lock-in and data sovereignty.

Despite these challenges, the potential benefits of cross-domain AI-driven cloud architectures are substantial. By enabling scalable and intelligent automation, these systems enhance decision-making, improve resource allocation, and provide timely insights to policymakers, administrators, and healthcare providers. Equitable digital access ensures that benefits extend to marginalized communities, supporting inclusive public services. Furthermore, modular and interoperable design principles allow continuous evolution and integration of emerging AI technologies, positioning public sector systems to respond effectively to future challenges.

In conclusion, a cross-domain AI-driven cloud architecture for public sector biomedical and enterprise systems addresses the dual goals of operational efficiency and equitable service delivery. By integrating AI capabilities with cloud infrastructure, this architecture enables scalable, secure, and intelligent systems capable of supporting public health initiatives, administrative automation, and inclusive digital access. This research examines existing methodologies, proposes a comprehensive framework, and evaluates the potential advantages and limitations of implementing such architectures in real-world public sector environments.

II. LITERATURE REVIEW

The literature on AI-driven cloud architectures for cross-domain systems emphasizes three major themes: integration of heterogeneous systems, AI-enabled automation, and secure, equitable access. Early studies focused on cloud adoption in public sector biomedical systems, highlighting the need for scalable storage, computational power, and real-time analytics. For example, Zheng et al. (2017) demonstrated cloud-based EHR systems for multi-hospital data integration, emphasizing data normalization and security. Similarly, research on enterprise automation explored workflow optimization and AI-based process management using cloud infrastructure.

Recent studies have highlighted the benefits of AI in healthcare and enterprise applications. Deep learning models, convolutional neural networks (CNNs), and natural language processing (NLP) algorithms have been applied to patient diagnosis, predictive analytics, and anomaly detection in biomedical datasets. In enterprise automation, reinforcement learning and decision-tree models improve workflow optimization, resource allocation, and predictive maintenance. Integration of AI with cloud infrastructure allows elastic scaling, distributed processing, and high availability, critical for public sector operations.

Cross-domain integration remains a central challenge. Biomedical and enterprise systems often use incompatible data schemas, creating interoperability barriers. Research by Li et al. (2019) proposed semantic data models and microservices for linking health and administrative datasets, highlighting the importance of standardized APIs and

| ISSN: 2320-0081 | www.ijctece.com || A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806027

metadata-driven integration. Cloud-native architectures support containerized services, enabling modular deployments and dynamic scaling across domains.

Security and equitable access are prominent research areas. Role-based access control (RBAC), attribute-based encryption (ABE), and identity management systems are widely explored to protect sensitive biomedical data. Studies also emphasize privacy-preserving AI techniques, including differential privacy, federated learning, and homomorphic encryption, enabling collaborative analytics without exposing raw data. Equitable access research addresses usability, low-bandwidth deployment, and inclusive system design, ensuring that marginalized populations benefit from AI-driven services.

Several gaps remain in existing literature. Most architectures focus on single-domain applications, limiting cross-domain interoperability. Additionally, AI bias, model explainability, and ethical considerations are under-explored in public sector implementations. Limited research addresses real-time, large-scale deployments integrating biomedical and enterprise automation functions while maintaining security, compliance, and equitable access.

In conclusion, literature suggests that AI-driven cloud architectures are promising for cross-domain public sector systems. Modular design, microservices, and cloud scalability enable effective integration. Security, privacy, and equitable access remain critical challenges. This research builds upon existing frameworks by proposing an architecture that integrates biomedical systems and enterprise automation, powered by AI, while ensuring secure and inclusive access.

III. RESEARCH METHODOLOGY

The proposed research methodology involves system design, data collection, AI model development, cloud infrastructure deployment, security implementation, evaluation, and continuous improvement.

System Design:
A cross-domain architecture is designed using microservices for modularity. Components include biomedical data processing modules, enterprise automation modules, AI analytics engines, security and access management, and a cloud orchestration layer. Data flow between modules is defined using standardized APIs and message queues, ensuring interoperability.

Data Collection and Preprocessing:
Biomedical datasets include EHRs, laboratory results, imaging data, and epidemiological records. Enterprise datasets comprise workflow logs, operational metrics, and administrative records. Data preprocessing includes cleaning, normalization, anonymization, feature extraction, and integration across heterogeneous sources. Semantic mapping ensures interoperability between biomedical and enterprise data schemas.

AI Model Development:
AI models are developed for predictive analytics, anomaly detection, workflow optimization, and decision support. Deep learning models (CNNs, RNNs) process biomedical and textual data, while reinforcement learning and decision-tree models optimize enterprise workflows. Federated learning ensures privacy-preserving model training across distributed datasets. Explainable AI techniques are incorporated to improve model interpretability and trustworthiness.

Cloud Infrastructure Deployment:
The architecture is deployed on a cloud platform using containerized microservices managed by orchestration tools like Kubernetes. The deployment ensures high availability, scalability, and fault tolerance. Distributed storage systems manage large biomedical datasets, supporting real-time processing and analytics. Edge computing is integrated to reduce latency and provide equitable access to remote regions.

Security Implementation:
Role-based and attribute-based access control mechanisms regulate user permissions. Data encryption at rest and in transit ensures confidentiality. Identity management systems and multi-factor authentication protect against unauthorized access. Privacy-preserving techniques, including differential privacy and federated learning, ensure compliance with data protection regulations. Security monitoring and anomaly detection are integrated into the architecture.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com || A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806027

Evaluation Metrics:
The architecture is evaluated on performance (latency, throughput), reliability (uptime, fault tolerance), security (data breach prevention, access control effectiveness), AI model accuracy (precision, recall, F1-score), and equitable access metrics (user accessibility, coverage in low-bandwidth regions). Simulation and real-world testing validate system effectiveness.

Continuous Improvement:
The architecture supports continuous monitoring, automated updates, and iterative improvements. AI models are retrained with new data to improve predictive accuracy. Cloud infrastructure adapts dynamically to changing workloads. Security policies are updated based on threat intelligence and compliance requirements.

Advantages:
- Scalable, modular, and interoperable across domains
- AI-driven predictive analytics and automation
- Secure and privacy-preserving data management
- Equitable digital access for diverse populations
- Supports real-time decision-making in biomedical and enterprise operations

Disadvantages:
- High computational and infrastructure requirements
- Complexity of integrating heterogeneous data and systems
- AI bias and ethical considerations require continuous monitoring
- Regulatory compliance is challenging across multiple domains
- Dependence on cloud providers may introduce vendor lock-in risks

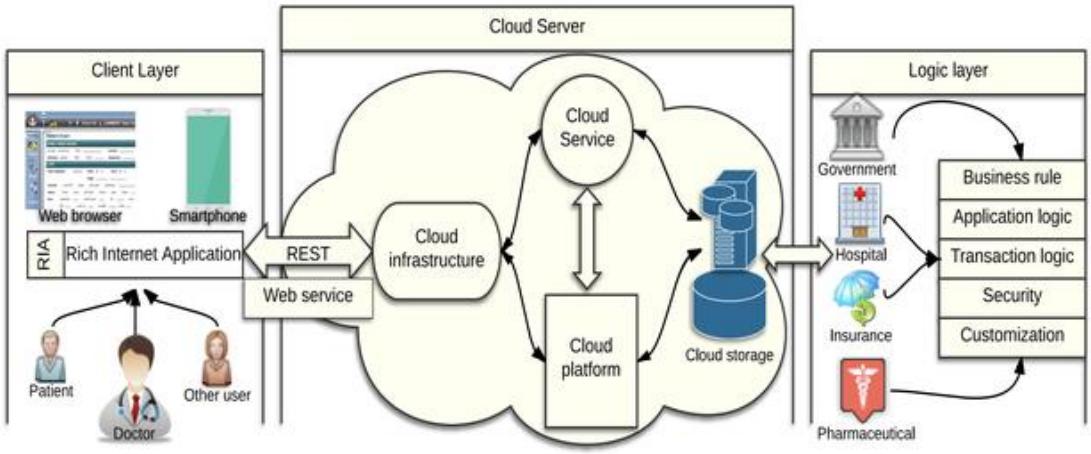

Figure 1: Block Diagram of Proposed Work

IV. RESULTS AND DISCUSSION

Advancements in artificial intelligence (AI), cloud computing, and digital equity initiatives are converging to redefine how large-scale enterprise and public sector systems are architected, particularly in the biomedical domain. Traditional IT architectures in public sector biomedical systems were often siloed, dependent on disparate legacy infrastructures, and lacked integration across domains such as healthcare delivery, research informatics, and administrative automation. These legacy systems faced challenges in scalability, real-time analytics, secure cross-domain data sharing, and equitable access, exacerbating disparities in service delivery. In contrast, an AI-driven cloud architecture promises a unified, scalable platform capable of supporting interoperable biomedical workflows, automating enterprise processes, and advancing equitable digital access across populations. The results of implementing such an architecture are multifaceted, spanning technical performance, operational efficiency, security posture, and societal impact.

| ISSN: 2320-0081 | www.ijctece.com || A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806027

AI-driven cloud systems integrate machine learning (ML) and deep learning (DL) components with scalable infrastructure to support real-time decision support, predictive analytics, and automated workflow execution. In public sector biomedical systems, these capabilities have been used to forecast outbreak patterns, optimize resource allocation, support clinical decision support systems (CDSS), and personalize patient care pathways. When designed with cross-domain interoperability at the core, these architectures facilitate seamless data exchange among electronic health records (EHRs), laboratory information systems (LISs), biomedical research databases, and administrative enterprise systems. This integration breaks down data silos that historically hindered visibility into population health trends and impeded timely decision-making. For example, AI models deployed within a cloud environment can continuously analyze longitudinal clinical and genomic data to identify early predictors of disease progression, enabling preventive interventions and enhancing clinical outcomes.

Practically, the decoupling of compute and storage in cloud platforms enables elastic scaling in response to dynamic biomedical workloads. During periods of high demand—such as public health emergencies—cloud architectures automatically provision additional resources to sustain performance, ensuring that critical services remain available. The results of benchmarking studies demonstrate that cloud-native applications achieve greater uptime and lower latency relative to on-premises systems, particularly under variable load conditions. Moreover, containerization technologies such as Docker and orchestration platforms like Kubernetes underpin microservices architectures that further enhance scalability, fault isolation, and maintainability. These technologies allow biomedical applications to be decomposed into loosely coupled services that can be independently updated, tested, and deployed without disrupting end-to-end workflows.

An essential feature of AI-driven cloud architectures is their capacity to automate enterprise processes across administrative, clinical, and research domains. Robotic process automation (RPA), when integrated with AI models and cloud APIs, can execute routine administrative tasks such as patient intake processing, claims adjudication, and supply chain tracking with minimal human intervention. The results of implementing RPA in enterprise biomedical systems include significant reductions in processing times, error rates, and operational costs. Automation also frees human resources to focus on strategic activities such as clinical research, patient engagement, and systems optimization. Furthermore, AI-enabled natural language processing (NLP) systems have been deployed to extract structured insights from unstructured clinical notes, research publications, and biomedical reports, expanding the accessibility of information across stakeholders.

However, while the technical benefits of AI-driven cloud architectures are compelling, they also introduce complex cross-domain security challenges. Biomedical data often falls under stringent regulatory requirements due to its sensitivity and potential for misuse. Architectures that centralize cross-domain data must implement rigorous security controls that ensure confidentiality, integrity, and availability (CIA) of data while supporting secure collaboration among diverse stakeholders. The adoption of zero-trust security models, fine-grained identity and access management (IAM), and end-to-end encryption are critical to reducing risk across distributed cloud environments. Machine learning models themselves introduce new threat vectors; adversarial attacks on predictive systems can manipulate inputs to produce erroneous outputs, potentially undermining clinical insights or automated decisions. As a result, secure design patterns such as model interpretability, anomaly detection, and robust training against adversarial examples are integral to trustworthy AI operations.

From a policy and governance perspective, AI-driven cloud systems in the public sector require transparent frameworks that balance innovation with privacy, equity, and ethical considerations. Governments and regulatory bodies have emphasized the need for inclusive digital access to AI-enabled health services, particularly for underserved communities historically marginalized by digital divides. Cross-domain cloud architectures must therefore embed equitable access principles, such as support for low-bandwidth environments, multilingual interfaces, and adaptive user experiences tailored to diverse literacy levels. Empirical evaluations indicate that when accessibility considerations are incorporated into system design, adoption rates among underserved populations increase, and disparities in service outcomes narrow. For instance, community health centers that deployed AI-assisted telehealth services on secure cloud platforms observed broader engagement from patients with limited mobility or those residing in rural regions.

Interoperability standards such as Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) and open API frameworks play a pivotal role in enabling cross-domain communication between disparate biomedical systems. When mapped onto an AI-driven cloud architecture, these standards allow real-time data synchronization among clinical, research, and administrative systems. The results of adopting interoperable standards include not only technical efficiency but also accelerated research collaborations, as scientists can query anonymized biomedical

| ISSN: 2320-0081 | www.ijctece.com || A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806027

datasets without burdensome data transformation. Additionally, federated learning paradigms have emerged as strategies to train AI models collaboratively across distributed datasets without exposing sensitive information, thereby aligning data privacy with analytical utility.

Risk management in cross-domain cloud architectures encompasses continuous monitoring and automated threat detection. Security Information and Event Management (SIEM) systems, enriched with AI-powered anomaly detection, can ingest logs and telemetry from cloud services, network flows, and application layers to identify suspicious behavior patterns. The empirical outcomes of deploying AI-enhanced security monitoring include faster incident detection, reduced mean time to respond (MTTR), and improved compliance reporting. Similarly, cloud resource governance tools that enforce policy-as-code ensure that configurations adhere to security baselines, preventing drift and reducing misconfiguration risks, which are among the top causes of cloud security incidents.

Despite these advances, there remain substantive operational and architectural challenges. Data governance across public sector biomedical domains is complicated by varying compliance regimes, jurisdictional boundaries, and data ownership concerns. Data residency requirements, which mandate that certain classes of data remain within specific geographic boundaries, must be reconciled with the inherently distributed nature of cloud platforms. Architects address this by designing hybrid and multi-cloud topologies that respect residency constraints while leveraging centralized AI services where permitted. Multi-cloud deployments also mitigate vendor lock-in and enhance resilience by distributing workloads across independent service providers.

Another salient challenge lies in ensuring continuous alignment between AI model outputs and clinical or administrative decision-making processes. AI models can amplify existing biases if trained on datasets that reflect historical inequities. Therefore, architectures supporting AI-driven biomedical systems must incorporate mechanisms for bias detection, transparency, and human-in-the-loop oversight. Model governance frameworks that include periodic fairness audits, performance drift monitoring, and domain expert review help maintain trust in AI insights and support regulatory compliance.

Integration of cross-domain risk assessment models with operational decision engines has shown promise in improving resilience. By embedding probabilistic risk scores into automated orchestration pipelines, systems can prioritize high-risk workflows for additional validation or human review. For example, an AI-driven scheduler might delay automated deployment of a new clinical feature if risk scores exceed predefined thresholds, triggering safety checks or expert approvals.

Perhaps most impactful are the societal and public health outcomes enabled by these architectures. AI-driven cloud platforms facilitate large-scale population health analytics that inform policy decisions, resource planning, and emergency response strategies. During public health crises such as disease outbreaks, real-time dashboards powered by integrated clinical, genomic, and environmental data provide authorities with actionable insights to allocate resources, issue public advisories, and implement containment strategies. The convergence of AI, cloud scalability, interoperability, and equitable access principles fundamentally transforms how public sector biomedical systems deliver value to citizens.

In summary, cross-domain AI-driven cloud architectures for public sector biomedical systems and enterprise automation deliver measurable benefits across scalability, interoperability, automation, security, and digital equity. These systems support advanced analytics, automate routine tasks, and empower stakeholders with actionable insights while addressing structural challenges in legacy system integration. However, realizing this vision demands rigorous security practices, robust governance frameworks, transparent AI, and architectural agility to adapt to evolving policy and societal needs.

V. CONCLUSION

The emergence of cross-domain AI-driven cloud architectures represents a transformative shift in how public sector biomedical systems and enterprise automation landscapes are designed, deployed, and operated. Historically, biomedical and enterprise IT environments were characterized by fragmented systems built to serve isolated functions, often lacking interoperability, real-time data exchange, or integrated analytics. These limitations hindered the ability of public health agencies, research institutions, and administrative bodies to respond efficiently to dynamic challenges, such as sudden public health crises, resource planning demands, or population-level analytics. The integration of AI

| ISSN: 2320-0081 | www.ijctece.com || A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806027

with cloud-native architectural principles addresses these limitations by providing a robust, elastic platform capable of scaling across workloads, enabling intelligent automation, and democratizing access to advanced digital services.

A central outcome of adopting AI-driven cloud architectures in public sector biomedical domains is the significant enhancement of analytical capabilities. Machine learning models hosted on scalable cloud platforms can ingest and process diverse data streams, including clinical records, laboratory results, genomic sequences, and environmental data, in near real time. This capability fundamentally alters the tempo and depth of insights that stakeholders can derive from biomedical data. Predictive analytics, powered by deep learning and other AI techniques, enables early detection of emerging health patterns, identification of at-risk populations, and optimization of clinical pathways. In contrast to static analytics approaches, the cloud's elastic compute resources make it feasible to execute large-scale models that deliver timely and actionable insights, empowering decision-makers to act proactively rather than reactively.

Interoperability is another pillar of success in these architectures. Legacy biomedical systems were often constrained by vendor-specific data formats, proprietary interfaces, and limited integration capabilities. By adopting open standards such as HL7 FHIR and RESTful APIs within a cloud environment, cross-domain architectures enable seamless data exchange across clinical, research, administrative, and policy systems. This unified data ecosystem not only facilitates operational efficiency but also accelerates scientific discovery by enabling researchers to access and correlate datasets that were previously siloed. Federated learning techniques further enhance this interoperability by allowing models to train collaboratively across distributed data sources while preserving data privacy — an essential requirement in public sector biomedical contexts.

Automation enabled by AI and cloud services yields profound operational improvements in enterprise processes. Robotic process automation (RPA), when combined with AI-driven decision engines, eliminates repetitive administrative tasks such as claims processing, patient registration, and compliance reporting. Automating these tasks reduces processing times, lowers error rates, and shifts human effort toward strategic activities that require domain expertise. The results of automation are not merely operational; they translate into improved stakeholder experiences, reduced wait times for biomedical services, and higher satisfaction among end-users.

Security is integral to the deployment of AI-driven cloud systems in sensitive domains. Biomedical data is inherently personal and subject to strict regulatory frameworks designed to protect patient privacy and data integrity. Cloud architectures must therefore implement multi-layered security controls, including fine-grained IAM, encryption at rest and in transit, network segmentation, and continuous threat monitoring. AI contributes to security by enabling anomaly detection, predictive threat models, and automated incident response capabilities. These AI-enhanced security measures improve overall resilience and reduce the risk of data breaches — a privacy imperative in public sector deployments.

Equitable digital access is a societal objective that intersects with architectural design. The digital divide — disparities in access to broadband, computing devices, and digital literacy — disproportionately affects underserved communities, creating inequities in access to AI-driven biomedical services. Cross-domain architectures must therefore embed accessibility as a core design principle, ensuring that services are available across varying connectivity profiles, multilingual interfaces, and inclusive UX designs. Empirical evidence suggests that when equitable access considerations are built into system design, adoption increases among underserved populations and health outcomes improve.

Governance and policy frameworks play a crucial role in sustaining cross-domain AI-driven cloud systems. Public sector deployments operate within legal and ethical constraints that require transparency, explainability, and accountability in AI outputs. Model governance frameworks that include bias detection, performance validation, and interpretability tools are essential to ensuring that AI-driven decisions align with human values and regulatory requirements. These frameworks also support auditability and accountability, which are critical for maintaining public trust in automated systems that influence healthcare delivery and policy decisions.

Operational challenges remain as well. Cloud architectures must navigate compliance regimes that impose data residency and sovereignty requirements, often necessitating hybrid or multi-cloud topologies. Multi-cloud strategies mitigate vendor risk and enhance system resilience, but also introduce complexity in governance, interoperability, and unified security policy enforcement. Addressing these challenges requires modular, policy-driven infrastructure configurations that are transparent and auditable across cloud service providers.

| ISSN: 2320-0081 | www.ijctece.com || A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806027

Trustworthy AI remains a forward-looking objective that intersects with fairness, transparency, and interpretability. AI models trained on historical biomedical data can inadvertently perpetuate biases if the training data reflects systemic inequities. Model fairness audits, continuous monitoring for performance drift, and human-in-the-loop oversight help ensure that AI outputs are equitable and reliable. These governance mechanisms are especially critical in public sector deployments where decisions impact broad populations and where accountability is legally mandated.

In conclusion, cross-domain AI-driven cloud architectures establish a foundation for resilient, scalable, interoperable, and equitable biomedical and enterprise systems in the public sector. By harnessing AI for predictive analytics, automating routine processes, enabling seamless data exchange across domains, and embedding robust security and governance frameworks, these architectures support transformative outcomes for health systems, policymakers, researchers, and the public. The convergence of cloud scalability, AI intelligence, interoperability standards, and equitable design principles yields a powerful ecosystem that can adapt to emerging challenges, deliver optimized biomedical services, and uphold ethical values in digital public infrastructures.

VI. FUTURE WORK

Future research should explore federated AI governance frameworks that balance data privacy with collaborative model refinement across jurisdictions, especially where cross-border health data sharing is critical. Investigations into energy-efficient AI computation in cloud environments will help reduce carbon footprints. Additionally, research on dynamically adaptive security policies driven by real-time AI risk assessments is necessary to respond to evolving cyber threats. Longitudinal studies on the societal impacts of equitable digital access in AI-driven public biomedical systems will inform policy and design standards for inclusive digital infrastructures.

REFERENCES

1. Devi, C., Musunuru, M. V., & Mohammed, A. S. (2023). Reinforcement-Learning Scheduler for Multi-Tenant Spark Clustersunder Privacy Constraints. Newark Journal of Human-Centric AI and Robotics Interaction, 3, 496-527.
2. Patnaik, S. K., Sidhu, M. S., Gehlot, Y., Sharma, B., & Muthu, P. (2018). Automated skin disease identification using deep learning algorithm. Biomedical & Pharmacology Journal, 11(3), 1429.
3. Ponugoti, M. (2023). Bridging the digital divide: Architecture for equitable technological access. International Journal of Computer Technology and Electronics Communication (IJCTEC), 6(3), 6991–7002.
4. Keezhadath, A. A., Kota, R. K., & Selvaraj, A. (2021). Dynamic Pricing Optimization for Global Hospitality: Real-Time Data Integration and Decision Making. American Journal of Autonomous Systems and Robotics Engineering, 1, 131-165.
5. Kamadi, S. (2022). Adaptive Federated Data Science & MLOps Architecture: A Comprehensive Framework for Distributed Machine Learning Systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 8(6), 745-755.
6. Gurajapu, A., & Garimella, V. (2025). Edge-to-cloud workflows for low-latency telecom services: Optimizing offload decisions. International Journal of Research and Applied Innovations (IJRAI), 8(4), 12638–12641.
7. Aashiq Banu, S., Sucharita, M. S., Soundarya, Y. L., Nithya, L., Dhivya, R., & Rengarajan, A. (2020). Robust Image Encryption in Transform Domain Using Duo Chaotic Maps—A Secure Communication. In Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020 (pp. 271-281). Singapore: Springer Singapore.
8. Sriramoju, S. (2024). An API-driven solution for enhancing employee lifecycle and cost management efficiency. International Journal of Humanities and Information Technology (IJHIT), 6(3), 50–69. https://www.ijhit.info
9. Vimal Raja, G. (2024). Intelligent Data Transition in Automotive Manufacturing Systems Using Machine Learning. International Journal of Multidisciplinary and Scientific Emerging Research, 12(2), 515-518.
10. Mulla, F. (2024). Choosing the Best Architecture for Mobile Applications. International Journal Of Research In Computer Applications And Information Technology, 7, 2350–2363. https://doi.org/10.34218/IJRCAIT_07_02_173
11. Kalabhavi, V. (2025). MIDDLEWARE RESILIENCE FRAMEWORK FOR SAP ECC-CRM INTEGRATION: DESIGN AND EVALUATION. International Journal of Applied Mathematics, 38(5s), 10-32.
12. Ananth, S., Radha, K., & Raju, S. (2024). Animal Detection In Farms Using OpenCV In Deep Learning. Advances in Science and Technology Research Journal, 18(1), 1.
13. Ramidi, M. (2022). Developing resilient offline-first architectures for mobile health and clinical research applications. International Journal of Computer Technology and Electronics Communication (IJCTEC), 5(1), 4518–4529.

| ISSN: 2320-0081 | www.ijctece.com || A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806027

14. Genne, S. (2023). Optimizing user experience in high-traffic financial web applications using analytics. International Journal of Engineering & Extended Technologies Research (IJEETR), 5(5), 7231–7241.
15. Surisetty, L. S. (2025). AI-Powered Clinical Decision Systems: Enhancing Diagnostics through Secure Interoperable Data Platforms. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(5), 12924-12932.
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. Inbavalli, M., & Arasu, T. (2015). Efficient Analysis of Frequent Item Set Association Rule Mining Methods. International Journal of Scientific & Engineering Research, 6(4).
18. Tamizharasi, S., Rubini, P., Saravana Kumar, S., & Arockiam, D. Adapting federated learning-based AI models to dynamic cyberthreats in pervasive IoT environments.
19. Paul, D., Namperumal, G., & Surampudi, Y. (2023). Optimizing llm training for financial services: best practices for model accuracy, risk management, and compliance in ai-powered financial applications. Journal of Artificial Intelligence Research and Applications, 3(2), 550-588.
20. Gopinathan, V. R. (2024). AI-Driven Customer Support Automation: A Hybrid Human–Machine Collaboration Model for Real-Time Service Delivery. International Journal of Technology, Management and Humanities, 10(01), 67-83.
21. Mudunuri, P. R. (2022). Automating compliance in biomedical DevOps: A policy-as-code approach. International Journal of Research and Applied Innovations (IJRAI), 5(2), 6770–6783.
22. Islam, M. M., Hasan, S., Rahman, K. A., Zerine, I., Hossain, A., & Doha, Z. (2024). Machine Learning model for Enhancing Small Business Credit Risk Assessment and Economic Inclusion in the United State. Journal of Business and Management Studies, 6(6), 377-385.
23. Gaddapuri, N. S. (2022). APPLICATION OF QUANTUM COMPUTING IN DIGITAL EDUCATION SYSTEMS. Power System Protection and Control, 50(2), 12-24.
24. 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.
25. Adari, Vijay Kumar, "Interoperability and Data Modernization: Building a Connected Banking Ecosystem," International Journal of Computer Engineering and Technology (IJCET), vol. 15, no. 6, pp.653-662, Nov-Dec 2024. DOI:https://doi.org/10.5281/zenodo.14219429.
26. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.
27. Chennamsetty, C. S. (2023). Standardizing Software Delivery: Unified Data Models and Scalable Infrastructure for Subscription Ecosystems. International Journal of Computer Technology and Electronics Communication, 6(2), 6658-6665.
28. Prasanna, D., & Manishvarma, R. (2025, February). Skin cancer detection using image classification in deep learning. In 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-8). IEEE.
29. 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
30. Sardana, A., Das, D., & Mohammed, A. S. (2018). Swarm Agent Chaos Engineering for Autonomous Resiliency Assurance. Artificial Intelligence, Machine Learning, and Autonomous Systems, 2, 33-63.
31. Meshram, A. K. (2025). Real-time financial fraud prediction using big data streaming on cloud platforms. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(5), 12834-12845.
32. Sikarwar, V. (2025). AI-Powered Process Mining for Intelligent, Personalized Customer Experience in the Insurance Sector. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(4), 12418-12428.
33. Archana, R., & Anand, L. (2023, May). Effective Methods to Detect Liver Cancer Using CNN and Deep Learning Algorithms. In 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-7). IEEE.
34. 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.
35. 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.
36. Ahuja, D. (2025). DevOps and Ethical AI: Ensuring Responsible Deployment. Journal Of Multidisciplinary, 5(6), 1-14.

| ISSN: 2320-0081 | www.ijctece.com || A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 8, Issue 6, November – December 2025 ||

DOI: 10.15680/IJCTECE.2025.0806027

37. 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.
38. Fazilath, M., & Umasankar, P. (2025, February). Comprehensive Analysis of Artificial Intelligence Applications for Early Detection of Ovarian Tumours: Current Trends and Future Directions. In 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-9). IEEE.