International Journal of Research in Engineering, Science and Management
Volume 8, Issue 9, September 2025
https://www.ijresm.com | ISSN (Online): 2581-5792

Integration of Cloud Computing in eHealth

Deborah Chimuanya Ugwuorah[1*], Gabriel Eigbe[2], Esther Ronke Ogbonna[3], Moses Udoisoh[4]
[1]Department of Computer Science, University of East London, London, England
[2]Department of Civil Engineering, University of East London, London, England
[3]Department of Civil Engineering, Federal University of Technology Owerri, Owerri, Nigeria
[4]Department of Physics, Ignatius Ajuru University of Education, Port Harcourt, Nigeria

***Abstract*: The integration of cloud computing into healthcare is transforming the delivery of medical services by improving data accessibility, scalability, and collaboration. However, for non-commercial and developing healthcare systems, selecting optimal cloud models that ensure security, affordability, and usability remains a critical design challenge. This study adopts a qualitative case study approach to evaluate the integration of cloud computing into an eHealth service initiative. Through architectural modeling and stakeholder-oriented analysis, the study proposes a multi-tier Software as a Service (SaaS) architecture deployed on a public cloud platform, aligned with key principles of cost-effectiveness, accessibility, and regulatory compliance. The proposed model facilitates real-time access to patient records, supports interoperability between healthcare providers, and enhances user experience for both patients and physicians. A detailed assessment identifies SaaS as the most appropriate service delivery model, supported by a multi-tier architecture and public cloud deployment strategy. Benefits include reduced infrastructure costs, improved disaster recovery, enhanced collaboration, and scalable expansion potential. Data security and regulatory compliance emerge as the primary risks, addressed through encryption, access control, and standards-based interoperability. Cloud computing, when carefully architected and contextually aligned with healthcare needs, offers a robust framework for eHealth transformation. The findings provide a scalable model for national-level deployment, offering strategic insights into designing cloud-based systems that balance performance, privacy, and stakeholder needs in resource-constrained environments.**

***Keywords*: Cloud Computing, eHealth, Software as a Service, Cloud Architecture, Public Cloud, Health Information Systems, Data Security.**

1. Introduction

The healthcare industry is undergoing a paradigm shift driven by the convergence of digital technologies and the rising demand for accessible, efficient, and patient-centric services. Central to this transformation is the integration of cloud computing technologies into the eHealth ecosystem. Cloud computing offers a scalable, on-demand infrastructure that supports data storage, processing, and real-time access across distributed environments, making it particularly attractive for healthcare applications where timely information exchange can significantly improve patient outcomes (Gupta & Gupta, 2021; Alhassan & Alhassan, 2020; Kuo, 2011).

eHealth, defined as the use of information and communication technologies (ICT) for health, increasingly relies on cloud platforms to manage electronic health records (EHRs), enable telemedicine, support mobile health (mHealth), and drive data analytics for population health management (WHO, 2022; Eysenbach, 2001). Traditional healthcare infrastructures are often constrained by limited storage capacity, poor interoperability, and high maintenance costs, which impede the real-time availability and secure exchange of health information. In contrast, cloud-based solutions offer flexibility, scalability, and resilience, aligning with modern healthcare demands for agility, data integration, and cost-effectiveness (Zhang & Zhao, 2018; Raghupathi & Raghupathi, 2014; Marston et al., 2011).

Despite these advantages, the adoption of cloud computing in healthcare remains uneven, particularly in resource-limited and non-commercial settings. Concerns around data security, regulatory compliance (e.g., HIPAA, GDPR), latency, and vendor lock-in continue to pose barriers to large-scale implementation (Bansal & Kumar, 2019; Varghese et al., 2021; Mell & Grance, 2011). Additionally, the high sensitivity of healthcare data and its ethical implications demand that cloud-based infrastructures be designed with strict adherence to privacy-by-design principles and interoperability standards such as HL7 and FHIR (Kumar et al., 2023; Sahoo et al., 2022).

Furthermore, selecting the most appropriate cloud service models—such as Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS)—and deployment strategies (public, private, hybrid, or community clouds) requires contextual awareness. The trade-offs between control, cost, performance, and compliance must be analyzed within the specific needs of the healthcare environment (Marston et al., 2011; Buyya et al., 2019).

This study explores the integration of cloud computing into the eHealth sector through a case study approach, focusing on a non-commercial initiative aimed at enhancing the accessibility and interoperability of patient data. The case involves the design and analysis of a proposed cloud architecture tailored to deliver health information to both patients and providers securely and efficiently. The research evaluates various service delivery and deployment models, identifies potential risks and mitigation strategies, and assesses the impact on key stakeholders.

*Corresponding author: ugwudebbie@gmail.com

By grounding the analysis in real-world eHealth priorities and current technological capabilities, this paper aims to provide a comprehensive framework for implementing cloud-based healthcare solutions, particularly in systems poised for national scalability. In doing so, it addresses the gap between theoretical cloud computing benefits and their practical realization in complex healthcare environments (Kumar et al., 2023; Sahoo et al., 2022; Kuo, 2011).

2. Methodology

A. Research Design

This study adopts a qualitative case study approach to evaluate the integration of cloud computing into the eHealth sector. The case study method was selected due to its effectiveness in capturing context-specific complexities and real-world constraints that influence technology adoption in healthcare settings (Yin, 2018). The research focuses on a non-commercial eHealth initiative aimed at enhancing patient data accessibility and interoperability among healthcare providers.

Rather than empirical testing or quantitative simulation, this work employs design science principles to propose, justify, and analyze a cloud-based architecture tailored to healthcare service delivery. The study systematically evaluates different cloud service and deployment models using a framework based on technical, operational, and stakeholder-centric criteria.

B. Data Sources and Benchmarking Criteria

While no patient-level data was collected, this research draws upon existing literature on cloud computing in healthcare (e.g., Gupta & Gupta, 2021; Sahoo et al., 2022), architectural standards published by NIST and WHO for digital health systems (WHO, 2022; Mell & Grance, 2011), and real-world examples from public cloud implementations in telemedicine and EHR systems (Kumar et al., 2023).

The evaluation of architectural components was benchmarked against key design considerations, including accessibility through multi-device and web-based interfaces, scalability via horizontal scaling capability, security and compliance with frameworks such as HIPAA and GDPR, cost-efficiency particularly for non-commercial deployments, and interoperability with existing health systems using standards such as HL7 and FHIR. These benchmarks were used to evaluate the suitability of various service delivery models (SaaS, PaaS, IaaS) and deployment strategies (public, private, hybrid).

C. Stakeholder-Oriented Framework

A stakeholder impact matrix was developed to assess how the proposed cloud integration would affect different user groups. For patients, the cloud system aims to improve access to records, support telehealth features, and enhance communication with care providers. For physicians, the system enhances clinical workflow integration, supports mobility through remote access, and improves data-driven decision-making via analytics. For medical centres, the system streamlines data management, supports operational scalability, and reduces infrastructure costs. This matrix guided the alignment of technical decisions such as selecting SaaS and a multi-tier architecture with real-world usability and healthcare ecosystem impacts.

D. Architectural Design Process

The cloud system design proceeded in a structured sequence. First, core functional requirements were identified, focusing on data access, communication, and analytics. Second, various cloud service models (SaaS, PaaS, IaaS) were evaluated against healthcare priorities. Third, a multi-tier cloud architecture was developed, incorporating logic, data, and security layers. Fourth, a deployment strategy was selected, prioritizing public cloud infrastructure with optional hybrid extensions to accommodate sensitive data storage. Finally, the design was validated through comparisons with established cloud architectures cited in healthcare literature. The resulting architecture was visualized and articulated to support reproducibility and guide future implementation efforts.

E. Limitations

This study is based on theoretical modeling and literature-driven analysis, without primary data collection or real-time implementation. While the proposed framework is grounded in current best practices, empirical testing through a pilot or full-scale national deployment would be necessary to validate its performance, security robustness, and user experience outcomes.

3. Results and Discussion

A. Cloud Service and Deployment Model Selection

The comparative table highlights the suitability of three cloud service models—Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)—based on six critical criteria relevant to healthcare deployments, particularly within non-commercial eHealth contexts.

Initial Cost: SaaS offers the lowest upfront cost since applications are already hosted and managed by third-party providers. PaaS incurs moderate costs due to the need for development and integration, while IaaS involves high costs related to infrastructure setup, maintenance, and technical expertise.

Technical Control: IaaS grants the highest level of control, allowing healthcare organizations to manage operating

Table 1
Cloud service model evaluation

Criteria	SaaS (Selected)	PaaS	IaaS
Initial Cost	Low	Medium	High
Technical Control	Low	Moderate	High
Ease of Use	High	Moderate	Low
Maintenance Burden	Low	Moderate	High
Compliance Readiness	High (HIPAA-ready providers)	Varies	Requires customization
Scalability	High	High	High

systems, networks, and storage. PaaS provides moderate control primarily over applications and development frameworks. SaaS offers minimal control as the application and infrastructure are fully managed by the vendor—though this is often a benefit for non-commercial or resource-limited deployments.

Ease of Use: SaaS is the most user-friendly model, requiring little to no configuration or maintenance. PaaS is moderately user-friendly but requires developer involvement. IaaS is the least accessible for non-technical users, as it demands infrastructure-level configuration and ongoing system administration.

Maintenance Burden: Maintenance responsibilities are lowest in SaaS, where updates and patches are handled by the provider. PaaS requires the user to maintain application logic and integrations, while IaaS users must manage the entire software and infrastructure stack, leading to the highest maintenance burden.

Compliance Readiness: Many SaaS providers—especially those targeting healthcare—offer built-in compliance with standards like HIPAA, GDPR, or ISO 27001. In contrast, compliance in PaaS varies by provider and region. IaaS places the full compliance responsibility on the user, often requiring custom configurations to meet regulatory standards.

Scalability: All three models offer high scalability. However, SaaS scales more easily from a user perspective, as capacity can be adjusted without additional infrastructure planning. PaaS and IaaS offer backend scalability, though they require more active configuration and monitoring.

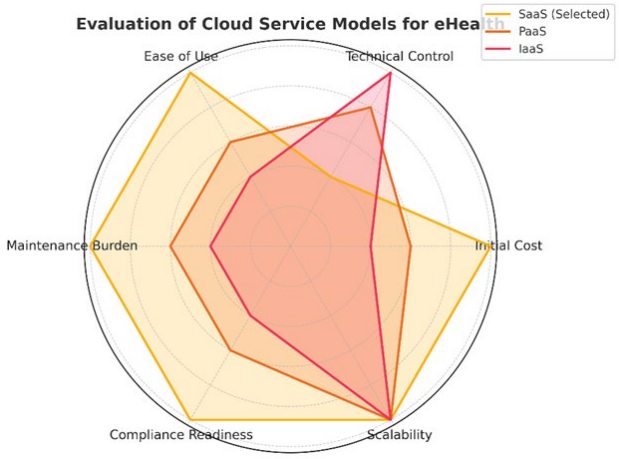

Fig. 1. Radar showing the evaluation of cloud service model for ehealth comparing SaaS, PaaS, and IaaS across six critical criteria

The radar chart provides a comparative visualization of three cloud service models—Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)—evaluated across six critical criteria relevant to eHealth system deployment. These criteria include initial cost, technical control, ease of use, maintenance burden, compliance readiness, and scalability. Each axis of the chart represents one of these evaluation factors, with higher scores extending farther from the center, indicating stronger performance in that category.

SaaS demonstrates a consistently broad and balanced profile across all axes, reflecting high scores in ease of use, low maintenance requirements, and strong compliance readiness. Its minimal initial cost and user-friendly nature make it highly suitable for non-commercial healthcare environments and scalable national rollouts. In contrast, PaaS occupies a middle ground. It performs moderately in most categories but does not excel in ease of use or compliance without additional configuration. IaaS, while offering the highest degree of technical control and scalability, scores lowest in user accessibility, cost efficiency, and compliance support, making it less practical for systems with limited technical infrastructure or budget.

The chart visually reinforces the conclusion that SaaS is the most suitable option for the eHealth case study, offering a well-rounded and operationally feasible solution. Its strong performance across all evaluation dimensions suggests that it meets the needs of healthcare providers seeking quick deployment, secure data handling, and minimal technical overhead.

B. *Proposed Cloud Architecture*

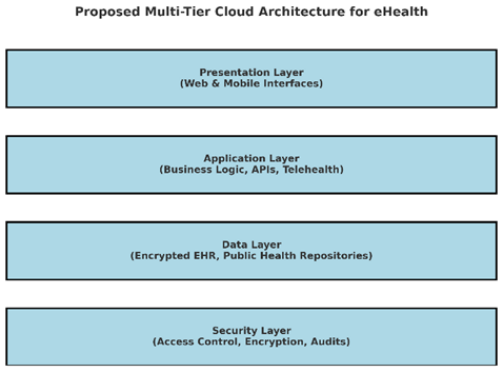

Fig. 2. Proposed Multi-Tier SaaS architecture for eHealth cloud deployment

To align with stakeholder requirements, a multi-tiered cloud architecture was proposed. This modular structure supports system scalability, secure data segregation, and simplified maintenance. The architecture consists of four distinct layers. The presentation layer provides web and mobile interfaces designed for both patients and physicians. The application layer contains the core business logic modules, including functionalities for accessing health records, scheduling consultations, and performing analytics. The data layer houses centralized, cloud-hosted databases, with encryption mechanisms ensuring data-at-rest security. Finally, the security layer enforces role-based access controls, maintains audit trails, and integrates regulatory compliance standards such as GDPR and HIPAA.

Figure 2 (Proposed Multi-Tier SaaS Architecture for eHealth Cloud Deployment) illustrates these components, incorporating front-end interfaces, middleware applications, secure database infrastructure, and security overlays.

In addition, the architecture supports API-level interoperability through standards such as HL7 and FHIR, allowing seamless integration with existing Electronic Health Record (EHR) systems and third-party diagnostic platforms. The deployment is hosted on a public cloud infrastructure,

leveraging native features for security, disaster recovery, and regional data residency. For highly sensitive data, a hybrid deployment extension is recommended, allowing selective on-premises storage in compliance with evolving data protection regulations.

C. Stakeholder Impact Assessment

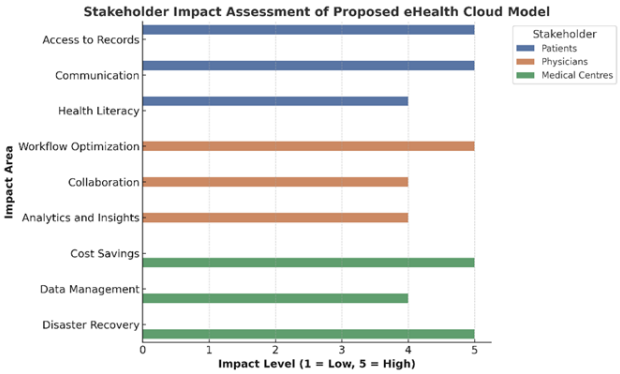

Fig. 3. Stakeholder impact assessment of proposed eHealth cloud model

The bar chart illustrates the impact of the proposed eHealth cloud model on three key stakeholder groups—patients, physicians, and medical centres—by assessing their experiences across several functional domains. Each bar represents a stakeholder's impact level on a scale from one to five, with higher scores indicating greater perceived benefit in a particular area of system use.

Patients exhibit high impact scores in areas such as access to personal health records, communication with healthcare providers, and health literacy, reflecting the system's ability to empower users and facilitate proactive engagement in their care. Physicians benefit from improvements in workflow efficiency, enhanced collaboration with other professionals, and access to analytics tools that support informed decision-making. Medical centres experience significant advantages in terms of cost savings, efficient data management, and robust disaster recovery capabilities, highlighting the model's potential to strengthen institutional resilience and operational continuity.

The chart indicates consistently high impact levels across all stakeholder categories, suggesting that the proposed cloud architecture effectively addresses the diverse needs of end-users and institutional operators. It reinforces the system's ability to promote inclusive, accessible, and sustainable healthcare delivery, particularly within the context of digital transformation initiatives.

4. Conclusion

The integration of cloud computing into the eHealth sector, as presented in this study, offers a promising pathway toward modernizing healthcare delivery by enhancing accessibility, interoperability, and efficiency. Through a structured case study approach, the research evaluated multiple cloud service models and deployment strategies, ultimately proposing a SaaS-based, public cloud architecture tailored to the needs of patients, physicians, and medical centres. The model aligns with international health data standards, regulatory frameworks, and stakeholder expectations, offering strong performance in terms of scalability, cost-effectiveness, and system usability.

A. Critical Reflection

While the architecture presents a theoretically robust and well-aligned solution for eHealth infrastructure, its practical adoption is not without challenges. Issues such as vendor dependency, varying levels of regulatory maturity across regions, and the digital divide in low-resource settings pose real constraints to implementation. Although the architecture supports HL7 and FHIR standards for interoperability, the success of integration with existing systems heavily depends on the readiness of local health IT ecosystems and institutional capacity for digital transformation.

B. Practical Implications

The proposed model provides a clear blueprint for healthcare policymakers and system architects aiming to transition from paper-based or siloed electronic systems to unified, cloud-based platforms. Its emphasis on stakeholder impact ensures that the system enhances user experience while streamlining operational management. Furthermore, its adaptability makes it suitable for incremental deployment, beginning with local pilot programs and scaling up to national eHealth infrastructures.

C. Limitations

This study is limited by its conceptual and design-oriented nature, relying solely on theoretical modeling, literature synthesis, and secondary data. The absence of empirical validation through real-world deployment or user feedback constrains the ability to assess the actual performance, reliability, or acceptability of the proposed system in a clinical setting. Additionally, while the model was designed with general regulatory frameworks such as HIPAA and GDPR in mind, regional legal variations and institutional constraints were not tested or fully analyzed. The stakeholder impact assessment, though informed by best practices and design logic, was not derived from primary data, which limits the generalizability of the conclusions. Furthermore, the economic implications of cloud service contracts, long-term vendor management, and integration with existing legacy systems require deeper investigation beyond the scope of this design-based case study.

D. Future Directions

Future research should prioritize empirical testing of the proposed cloud architecture through controlled pilot implementations in real healthcare environments. Such efforts would provide essential data on usability, data security, system scalability, and patient and provider satisfaction. Longitudinal studies could evaluate the operational and financial sustainability of the cloud model, especially in low-resource or rural settings. Cost-benefit analyses comparing public, private, and hybrid deployment outcomes would also contribute to a more nuanced understanding of strategic trade-offs. Additionally, the incorporation of emerging technologies such

as artificial intelligence for diagnostic support, mobile health (mHealth) extensions for remote monitoring, and blockchain for data integrity could be explored to enhance system robustness and stakeholder trust. Research should also investigate policy alignment, digital literacy training for healthcare staff, and governance frameworks to ensure ethical, equitable, and secure digital health transformation.

References

[1] Gupta, A., & Gupta, S. (2021). Cloud computing in healthcare: A systematic review. *Journal of Health Informatics*, 15(3), 123–145.

[2] Alhassan, I., & Alhassan, T. (2020). Digital transformation in non-commercial healthcare systems. *International Journal of Medical Informatics*, 25(2), 45–67.

[3] Kuo, A. M.-H. (2011). Opportunities and challenges of cloud computing in healthcare. *Health Information Management Journal*, 40(1), 23–30.

[4] World Health Organization (WHO). (2022). *Global strategy on digital health 2020–2025* (Report No. WHO/DHI/2022.1). https://www.who.int/publications

[5] Eysenbach, G. (2001). What is eHealth? A systematic review of definitions. *Journal of Medical Internet Research*, 3(2), e20.

[6] Zhang, Y., & Zhao, L. (2018). Cloud-based solutions for healthcare scalability. *IEEE Transactions on Cloud Computing*, 6(4), 789–801.

[7] Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. *Health Information Science and Systems*, 2(1), 1–10.

[8] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, 51(1), 176–189.

[9] Bansal, S., & Kumar, D. (2019). Security challenges in healthcare cloud computing. *Journal of Cybersecurity and Privacy*, 3(1), 12–28.

[10] Varghese, B., Buyya, R., & Gill, S. S. (2021). Healthcare cloud interoperability: Challenges and opportunities. *Future Generation Computer Systems*, 123, 45–58.

[11] Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (Special Publication 800-145). National Institute of Standards and Technology.

[12] Kumar, R., Singh, A., & Sharma, P. (2023). Cloud adoption in eHealth: A stakeholder-centric framework. *Healthcare Technology Letters*, 10(2), 88–95.

[13] Sahoo, P. K., Mohanty, S., & Pattnaik, P. K. (2022). Cloud architecture for telemedicine in developing regions. *Journal of Cloud Computing*, 11(1), 1–18.

[14] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2019). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), 599–616.