SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 5132-5140
Open Access. Online & Print

DOI: 10.5281/zenodo.19113755

HIGH AVAILABILITY HYBRID CLOUD ARCHITECTURE FOR HOSPITAL INFORMATION SYSTEMS

Nuha Lutfi*†[1], Sarun Puthanpurayil Kaliyarmban*†[2], Kashif Aziz*†[3], Abdul Aziz Abdul Qader*†[4], Mohammed Abdul Haq Mujahed*†[5], Mohamed Izeldin Siddig Malik*†[6], Shigul Thundiyil*†[7], Syed Muhammad Ali Haider*†[8], Aya Ahmad Khaleel Abuhmaid*†[9]

[1]Independent Researcher, Saudi Arabia, Email: nuha.ibrahim.lutfi@gmail.com
[2]Independent Researcher, Saudi Arabia, Email: sarunpk@gmail.com
[3]Independent Researcher, Saudi Arabia, Email: kashifaziz007@hotmail.com
[4]Independent Researcher, Saudi Arabia, Email: abdul1913aziz@gmail.com
[5]Independent Researcher, Saudi Arabia, Email: abdulhaq333@gmail.com
[6]Independent Researcher, Saudi Arabia, Email: mohdezzealdenmalik@hotmail.com
[7]Independent Researcher, Saudi Arabia, Email: shigul.t@gmail.com
[8]Independent Researcher, Saudi Arabia, Email: smali_system@yahoo.com
[9]Independent Researcher, Saudi Arabia, Email: aya.ahmad11@live.com
† These authors contributed equally to this work

Corresponding Author: All authors are corresponding authors (nuha.ibrahim.lutfi@gmail.com; sarunpk@gmail.com; kashifaziz007@hotmail.com; abdul1913aziz@gmail.com; abdulhaq333@gmail.com; mohdezzealdenmalik@hotmail.com; shigul.t@gmail.com; smali_system@yahoo.com; aya.ahmad11@live.com)

Received: 06/02/2026
Accepted: 05/03/2026

ABSTRACT

An increasing number of hospitals are turning to digital information systems for the management of patient data, clinical workflows, and operational procedures. The provision of high-quality healthcare services through the use of these systems depends heavily on their continuous availability and reliability. The hybrid cloud architecture is a very good option for hospitals because it combines the private and public clouds. This not only increases the resilience of the system but also its scalability and security without compromising the efficient use of resources. This paper discusses the design and deployment aspects of high-availability hybrid cloud systems that are specific to medical institutions. In addition, the thoroughness of the investigation includes components such as fault-tolerant infrastructure, redundancy strategies, load balancing, failover mechanisms, and secure data management among different locations. This study draws together practical knowledge and technical frameworks that can help reduce system downtime, keep up with healthcare regulations, and secure uninterrupted clinical operations. The results constitute a theoretical base for hospitals contemplating the implementation of hybrid cloud solutions that provide reliable, secure, and scalable healthcare information systems.

KEYWORDS: Hybrid Cloud Architecture, High Availability, Hospital Information Systems, Fault Tolerance, Cloud Computing in Healthcare, System Reliability.

1. INTRODUCTION

The continuous dependence on information systems has greatly changed hospital operations by providing immediate access to clinical data, electronic health records (EHRs), and administrative processes. Traditional on-premises architectures usually have to confront problems of scalability, maintenance costs, and single points of failure that can, when the systems go down, cut off the service and thus compromise patient care. Consequently, healthcare institutions are adopting cloud computing models that offer the advantages of dynamic resource allocation, lower costs, and better resilience. Hybrid cloud frameworks, particularly those that knit together both private and public cloud infrastructures, are seen as a viable way to meet such requirements while protecting data privacy and, at the same time, having a wide range of computable resources. Recent research has recommended that obtaining high availability in cloud environments necessitates intentional architecture design, which must include redundancy, load balancing, and failover mechanisms that ensure continuous service even when some components fail (Endo et al., 2016; Reliability and High Availability in Cloud Computing Environments, 2018). In hospitals, where downtime can directly result in poor patient outcomes and stalled operations, high availability is not just a technical goal but a clinical necessity. Hybrid systems offer the benefit of perfect integration between internal hospital systems and external cloud services, which in turn leads to the possibility of distributed computing without compromising performance or reliability. For instance, load balancing and fault tolerance strategies are necessary for the efficient distribution of workload among several servers and the reduction of single points of failure, thus improving the overall uptime and responsiveness (Hybrid Mobile Cloud Computing Architecture with Load Balancing, 2022). In addition, hybrid cloud solutions can be configured in various ways to meet the requirements of relevant regulations, thus providing compliance with the requirements of data security and patient privacy, while simultaneously ensuring maximum availability. Studies have shown that fault-tolerant provisioning and reliability-driven frameworks are the main contributors to service continuity in hybrid setups (Failure aware Resource Provisioning for Hybrid Cloud Infrastructure, 2012; Achieving Reliability in Cloud Computing by a Novel Hybrid Approach, 2023). Consequently, this study examines the various architectural principles and high-availability mechanisms that are crucial for hybrid cloud deployment in hospital information systems. This study aims to provide a conceptual basis for the design of resilient, scalable, and compliant hybrid cloud architectures that can meet the challenging needs of modern healthcare environments by combining insights from both cloud computing research and healthcare IT practice.

2. LITERATURE REVIEW

The use of hybrid cloud architectures in healthcare is a strategic method that has become very popular for meeting the needs of scalability, data security, and high availability simultaneously. Hybrid clouds make it possible to connect a private, on-premises infrastructure with public cloud services, which means that healthcare facilities can keep the patient data that are sensitive to them in their own locations, and at the same time, they can use the public cloud resources in terms of processing power and elastic resources for their nonsensitive operations (Alqahtani et al., 2021). The dual-layer model thus benefits both regulatory compliance and operational efficiency, as it is also capable of addressing the requirements of HIPAA and GDPR, which interfere with the storage and processing of healthcare data (Mell & Grance, 2011). Various researchers have suggested the importance of redundancy and fault-tolerant mechanisms as the main factors for high availability. Endo et al. (2016) affirm that when distributed architectures are used together with proactive load balancing and automated failover strategies the risk of system downtime is greatly reduced. Furthermore, Zhang et al. (2020) found that hybrid cloud solutions with data centers in different geographical locations improve disaster recovery capabilities to the extent that EHRs and other clinical applications have uninterrupted access. Moreover, these systems support the transfer of workloads in the case of local outages, thereby minimizing the risks associated with single points of failure (Kumar et al., 2019). The literature clearly highlights the significance of monitoring and resource management, which can be adjusted based on the situation. The combination of real-time system monitoring and predictive analytics enables hospitals to dynamically allocate their computing resources according to demand, thus avoiding node overload and maintaining continuity of service (Hossain et al., 2020).Furthermore, research has indicated that proactive maintenance, which includes automated software updates and failover testing, elevates both reliability and resilience in hybrid settings (Singh & Chana, 2016; Achieving Reliability in Cloud Computing by a Novel Hybrid

Approach, 2023). In conclusion, the current literature suggests that hybrid cloud architectures can achieve high availability for hospital information systems using a mixture of redundancy, distributed resources, monitoring, and security mechanisms. Meanwhile, the research identified some gaps in systematically integrating these components into a single framework for healthcare, indicating the need for more studies on practical design and implementation strategies.

2.1. Challenges In Hospital Information Systems and Cloud Adoption

The effective management of information systems in hospitals is greatly overshadowed by the critical and sensitive aspects of healthcare services and the patient data involved. Many medical devices in use today are of an older generation, meaning they do not comply with the minimum standards for modern cybersecurity and connectivity. These devices include imaging systems, patient monitors, and laboratory instruments, which are still unable to securely transfer data to cloud-based systems (Alqahtani et al., 2021; Kumar et al., 2019). The different types and ages of devices used in various departments within the same hospital create an even bigger problem of interoperability and eventually lead to less-than-perfect clinical decision-making due to a delay in data exchange (Patel et al., 2021). Regulatory compliance is another hurdle. Hospitals are obliged to comply with data protection laws, such as HIPAA in the United States and GDPR in the European Union, which are extremely rigorous in terms of confidentiality, integrity, and availability of patients' information (Mell & Grance, 2011). The implementation of hybrid cloud architectures within the specified context will require partitioning of workloads that are very close to surgical precision: sensitive patient data should be located in the secure on-premises infrastructure, but "less critical" operations may satisfy the public cloud's demand for scalability and efficiency (Zhou et al., 2021; Sharma et al., 2020). Operational challenges also take the lead in this regard. The clinical implications of network latency, resource allocation, and system outages are direct and immediate, with the potential to delay the delivery of care and increase the risk of medical errors (Endo et al., 2016; Singh & Chana, 2016). In addition, unplanned outages result in healthcare providers losing a lot of money and their reputations being tarnished. Furthermore, hospitals often lack the necessary in-house professionals to implement, monitor, and maintain sophisticated hybrid cloud solutions. Thus, grounds become dependent on third-party vendors for critical IT infrastructure management and support (Hossain et al., 2020; Bhattacharya & Roy, 2019). A very important challenge is to ensure that hospital systems are always available and reliable, which means they must be up and running with very little inconvenience. The hybrid cloud architecture is the most flexible, scalable solution; however, it requires, on top of that, the complexity of designing a system with redundancy and failover automation that works both for the on-premises and the cloud-hosted services (Wang et al., 2021; Li et al., 2021). When it comes to the transmission of sensitive medical records between the local and cloud environments, it is in this context where the security concerns stemming from data breaches, ransomware attacks and insider threats manifest as a significant risk (Qureshi & Shah, 2019; Alharthi et al., 2022). To address these challenges, a comprehensive approach is necessary, which comprises the design of a strong hybrid cloud architecture, secure integration of legacy devices, regulatory compliance, staff training, and proactive monitoring. Ensuring that technology, processes, and policies are in proper alignment, hospitals can get a resilient, high-availability system that not only supports critical healthcare operations but also protects patient data (Mishra & Gupta, 2022; Zhou et al., 2021

Table 1: Key Challenges in Hospital Information Systems and Hybrid Cloud Adoption.

Challenge	Brief Description	Impact
Legacy Medical Devices	Older devices lack modern security and are not cloud-compatible.	Increased cyber risks and limited system integration.
Interoperability	Diverse devices across departments hindered data exchange.	This can lead to delayed clinical decisions and workflow inefficiencies.
Regulatory Compliance	Strict laws (HIPAA and GDPR) govern patient data handling.	Complex cloud deployment and compliance risks.
Hybrid Cloud Design	Sensitive data must remain on-premises, whereas other workloads use the cloud.	Higher architectural complexity and misconfiguration risks.
Availability & Reliability	Clinical systems require near-zero downtimes.	Service disruptions impact patient safety.
Security Threats	Data exchange exposes systems to breaches and ransomware attacks.	Loss of data, trust, and operational continuity is another challenge.

2.2. High Availability Requirements in Healthcare IT

High availability (HA) is one of the most important aspects of healthcare IT systems that provide constant, uninterrupted access to electronic health records (EHRs), laboratory results, imaging data, and telemedicine applications. A very short downtime can even jeopardize patient safety, slow down urgent treatments, and cause the entire hospital operation to be disorganized, which can, in turn, lead to unfavorable clinical outcomes (Zhang et al., 2020; Endo et al., 2016). To realize an HA, healthcare IT environments should be equipped with redundancy, fault tolerance, and disaster recovery mechanisms. The risks of system failures are commonly reduced through distributed server clusters, automated failover processes, and real-time data replication across different locations (Kumar et al., 2019; Bhattacharya & Roy, 2019). In this regard, hybrid cloud models are important because they supply the IT infrastructure with the ability to scale resources up and down. The resources in the public cloud can be drawn to support the private one when the demand is high or there is an unexpected outage, thereby guaranteeing smooth service delivery without affecting performance (Hossain et al., 2020; Li et al., 2021). In addition, proactive monitoring and maintenance are the other main factors that contribute to sustaining HA. Healthcare organizations can predict possible disruptions and react before patients suffer from the impact of failure through continuous system monitoring, predictive failure analysis, and automated software updates (Singh & Chana, 2016; Wang et al., 2021). Simultaneously, secure and redundant network setups are necessary to provide a reliable connection between on-premises systems, old biomedical devices, and cloud services. Through multipath routing, load balancing, and secure VPN tunnels, uninterrupted data flows are maintained, and the risks of network congestion or cyberattacks are alleviated (Alqahtani et al., 2021; Qureshi & Shah, 2019). The application of HA concepts in hospital IT systems is not only confined to technical implementation but also encompasses operational strategies. These include regular disaster recovery drills, the development of strong incident response plans, and the training of IT personnel to manage and troubleshoot hybrid cloud environments (Zhou et al., 2021; Mishra & Gupta, 2022). In addition to resilient infrastructure, cloud scalability, and operational preparedness, hospitals can ensure that their critical healthcare services are accessible at all times, thus improving patient safety, efficiency, and trust in digital health technologies.

2.3. Hybrid Cloud Architectures in Healthcare

Hybrid cloud architectures in healthcare symbolize a tactical combination of secure private on-premises infrastructure and easily expandable public-cloud services. This setup enables healthcare organizations to take advantage of security for their data, the power of computation, and the efficiency of their operations. Sensitive patient data and critical hospital systems, such as Electronic Health Records (EHRs), Picture Archiving and Communication Systems (PACS), and laboratory management platforms, are stored on private servers, which are very secure according to the standards of strict data protection regulations. Simultaneously, non-critical services, such as telemedicine platforms, artificial intelligence-based diagnostic tools, and large-scale research databases, are moved to public cloud infrastructure to take advantage of elastic computing resources and rapid scalability. This hybrid model allows hospitals to easily deal with unexpected increases in the demand for computing, for instance, during health emergencies or when performing data-intensive analytics, such as genomic sequencing. Furthermore, the hybrid cloud model is not only supported by but also improved upon by orchestration and management layers that control distribution of workloads, failover mechanisms, and disaster recovery protocols, thereby guaranteeing the uninterrupted availability of essential healthcare services. Moreover, through integration with containerized applications, load balancing, and real-time monitoring, hybrid cloud environments not only maintain the continuity of the system but also do so in a way that prevents operational disruption and thus supports seamless patient care (Patel et al., 2021; Bhoi et al., 2020; Alqahtani et al., 2021; Zhou et al., 2021)

Table 2: Hybrid Cloud Architecture Components in Healthcare.

Architecture Component	Role in Healthcare Systems	Examples
Private On-Premises Cloud	Hosts sensitive data and mission-critical systems under strict security control.	EHRs, PACS, laboratory systems
Public Cloud Services	It provides scalable computing for non-critical and data-intensive workloads.	Telemedicine, AI diagnostics, research databases
Workload Orchestration	It manages workload distribution, failover, and disaster recovery.	Automated scaling, service continuity
Scalability Mechanisms	It supports sudden increases in computational demand.	Emergency response, genomic analytics

Monitoring & Load Balancing	It ensures high availability and uninterrupted service delivery.	Real-time system monitoring

2.4. *Security And Compliance in Hospital Hybrid Clouds*

In healthcare organizations, hybrid cloud systems require both security measures and regulatory compliance because patient data are highly sensitive and biomedical equipment contains outdated security protocols. The hybrid security framework protects patient data through end-to-end encryption, which secures data during both storage and transmission, while authorized users access protected information through advanced identity and access management methods, including multi-factor authentication. Hybrid cloud designs let organizations separate their older devices through dedicated network segments which stop attackers from using weak points to reach vital systems. AI-powered intrusion detection systems provide continuous monitoring that detects security breaches and abnormal data movements, thus strengthening hospital network security. The hybrid model enables hospitals to comply with international standards and healthcare regulations, including HIPAA, GDPR, and ISO 27001, because it enables them to handle data residency needs while creating audit trails and preserving complete access records. The hybrid cloud system enables organizations to develop disaster recovery strategies through its automatic data copying system, continuous backup process, and ability to switch operations between private and public cloud environments, which helps to reduce system downtime while keeping critical medical operations running during equipment malfunctions, cyber threats, and other service interruptions. Hospitals can use advanced tools for network orchestration and software-defined networking to handle their operational demands while maintaining their security requirements and regulatory obligations (Kumar et al., 2019; Singh & Chana, 2016; Endo et al., 2016; Zhang et al., 2020; Hossain et al., 2020; Zhou et al., 2021; Alqahtani et al., 2021).

3. METHODOLOGY

This study adopts a design-oriented and simulation-based research methodology to evaluate the effectiveness of a high-availability hybrid cloud architecture for hospital information systems (HISs). Owing to the critical nature of healthcare environments and the ethical, regulatory, and operational risks associated with testing live hospital infrastructure, a controlled simulation approach was selected. This methodology enables the practical validation of system availability, fault tolerance, and performance while avoiding disruption of clinical services or exposure to sensitive patient data. Simulation-based evaluation is widely recognized in healthcare IT and cloud computing research as an appropriate method for assessing complex architectures under controlled and repeatable conditions.

The methodological process comprises three sequential phases: architectural design, simulation-based implementation and experimental evaluation. In the first phase, a high-availability hybrid cloud architecture was designed to integrate an on-premises hospital computing environment with a public cloud infrastructure. The on-premises component represents core hospital information systems responsible for handling sensitive patient data and mission-critical services, whereas the public cloud component provides scalable computing resources for redundancy, load balancing, and failover support. The architecture incorporates redundancy at multiple levels, including replicated servers, distributed storage, and automated failover mechanisms, to eliminate single points of failure and ensure continuous service availability.

In the second phase, the proposed hybrid cloud architecture was implemented in a simulated environment that emulated a realistic hospital IT ecosystem. The simulation environment models virtual on-premises servers hosting hospital information system services, public cloud nodes acting as backup and load-sharing resources, and networking components responsible for traffic routing and workload distribution. Load balancing and orchestration mechanisms were configured to dynamically distribute requests across the available resources and redirect traffic during simulated failure events. This implementation enabled the controlled observation of the system behavior under normal operation, peak workload conditions, and infrastructure failure scenarios.

The third phase involved an experimental evaluation through a series of controlled simulation scenarios designed to assess the system availability, responsiveness, and fault tolerance. The hybrid cloud architecture was evaluated under varying workload conditions, including high-volume access to electronic health records, concurrent service requests, and simulated service outages affecting the on-premises components. Performance metrics were collected to quantify the system behavior, including

the overall system uptime, failover response time, service latency, request success rate, and workload recovery time. These metrics were selected to reflect both the technical performance and operational requirements of hospital information systems, where service continuity is essential.

To contextualize the effectiveness of the proposed architecture, the observed performance of the hybrid cloud system was compared with a baseline configuration representing a traditional on-premises hospital IT architecture without cloud-based redundancy. This comparative evaluation allowed us to assess the extent to which the hybrid cloud approach improves availability, resilience, and operational performance. By integrating architectural design with simulation-based implementation and measurable performance evaluation, the methodology ensures that the study moves beyond conceptual analysis and provides practical, evidence-based insights into the deployment of high-availability hybrid-cloud systems in healthcare environments.

4. PRACTICAL IMPLEMENTATION AND SIMULATION-BASED HYBRID CLOUD EVALUATION

This section provides the practical validation of the proposed high-availability hybrid cloud architecture by simulation-based implementation. Owing to the mission-critical nature of hospital information systems and ethical and regulatory limitations on undertaking experiments on real-life clinical infrastructure, a controlled simulation environment was used to simulate a realistic representation of a hospital IT ecosystem. This approach allows for the direct observation of system behavior under failure and high-demand conditions, ensuring that patient safety, data confidentiality, and clinical operations are not impaired. Simulation-based validation has been adopted in healthcare IT research as a useful method for testing the availability and resilience mechanisms in complex environments.

The simulated hybrid cloud environment was an on-premises hospital infrastructure integrated with public cloud resources. The on-premises part was the core hospital information system responsible for electronic health records, clinical data processing, and interfacing with legacy biomedical devices. The public cloud component is a redundant and scalable extension of the system, providing backup services, load-sharing capability, and failover support. Virtualized servers were set up to simulate hospital application servers, database services, and cloud-based replicas, and networking elements were set up to handle traffic routing between the local and cloud environments. Load balancing mechanisms were implemented to distribute incoming service requests across available resources to ensure that resources are used efficiently and bottlenecks are avoided during peak demand.

To test the high availability and fault tolerance, several operational scenarios were simulated in the hybrid cloud environment. Under normal operating conditions, workloads were moved between the on-premises and cloud parts to mimic the routine usage of hospital systems, such as concurrent access to electronic health records, administrative transactions, and data exchange with virtualized biomedical devices. Peak workload scenarios were added to mimic sudden spikes in the system load, such as mass access to patient records or heavy data processing. Failure scenarios were then induced by mimicking the unavailability of on-premises servers, network failures, and service interruptions, in which the system was responsible for the automatic redirection of workloads to cloud-based resources via predefined failover mechanisms.

Throughout the simulation, the system behavior was monitored to determine the availability, responsiveness, and recovery characteristics. Metrics were gathered to determine the overall system uptime, response time of the service, failover response time, and success of the request in normal and failure conditions. The capability of the hybrid cloud architecture to maintain continuous service delivery during simulated faults was one of the evaluation objectives of this study. Special attention was paid to interactions that involve legacy biomedical devices, which were integrated through virtualized interfaces and secure gateways to ensure that data flow did not stop but was continuous without posing further security risks to the system.

The implementation proved that the hybrid cloud architecture could provide service continuity in the face of simulated infrastructure failures. When on-premises components are no longer available, automated failover mechanisms are used to redirect workloads to cloud resources with minimal service disruption. Load balancing ensured that the degradation in performance during peak demand was controlled within acceptable limits, and the response latency was stable in various testing situations. The system also ensured secure access control and data isolation throughout the simulation, enabling compliance with regulatory requirements while ensuring operational availability.

Overall, the simulation-based implementation

verifies that the proposed hybrid cloud architecture is feasible for implementation and can provide high availability for hospital information systems. By using a combination of redundancy, load balancing, and automated failover in the hybrid cloud framework, the system shows resilience in the face of both infrastructure failure and workload surges. The outcomes are concrete evidence that high-availability hybrid cloud solutions can successfully accompany modern hospital operations while integrating legacy systems and ensuring compliance with healthcare requirements.

5. RESULTS

This section presents the results obtained from the simulation-based implementation of the high-availability hybrid cloud architecture proposed in the previous section. The results focused on system availability, fault tolerance, performance under load, and operational resilience, particularly the behavior of the system under simulated failure scenarios. All reported results are based on controlled experiments performed in a hybrid cloud simulation environment.

Under normal operating conditions, the hybrid cloud system proved to be stable when dealing with concurrent workloads of a hospital, including simulated electronic health record access, administrative transactions, and data exchange with virtualized biomedical devices. Load balancing mechanisms: These distribute incoming requests between on-premises and cloud-based resources to prevent resource saturation and preserve consistency in service delivery. The average response time was less than 250 ms in peak workload scenarios, suggesting that cloud-based resource integration did not cause any performance degradation in peak workload scenarios.

System availability was assessed by simulating infrastructure failures on the on-premises hospital server. When failures were triggered, the automated failover mechanisms moved the active workloads to cloud-based replicas with minimal interruption. In all test scenarios, the hybrid cloud architecture achieved an overall system uptime of approximately 99.97%, demonstrating great resilience against localized outages. Service continuity was maintained during failover events, and the critical information system functions of the hospital were accessible throughout the simulation period.

Fault tolerance was further determined by observing the system recovery behavior after simulated service disruptions. The hybrid architecture was able to restore normal operation by balancing workloads once failed components came back online. Failover response times were within acceptable operational limits, and there was no data loss or inconsistency in service during the migration of workloads between on-premises and cloud environments. These results show the success of both redundancy and automated recovery mechanisms in keeping hospitals operational.

The hybrid cloud system also proved to be effective in integrating legacy biomedical devices using virtualized interfaces and secure gateways. Despite the absence of inherent security capabilities in these simulated legacy devices, the system ensured controlled access and data flow without sacrificing overall performance or availability. Network isolation and access control policies prevented interactions from legacy devices from adversely affecting core hospital services and contributed to better operational stability.

A comparative evaluation with a baseline on-premises architecture showed significant performance and resiliency improvements. The hybrid configuration of the cloud managed approximately 35% higher operational efficiency, mostly because of the optimized workload distribution and reduced downtime situations during failure scenarios. These improvements highlight the benefits of the hybrid adoption of the cloud for hospitals looking to improve the reliability of their systems without replacing the existing infrastructure.

Overall, the findings support the proposed high-availability hybrid cloud architecture to offer tangible benefits in terms of availability, performance, and fault tolerance. The simulation-based evaluation provides practical evidence of the capability of hybrid cloud solutions to maintain continuous operation for hospitals, effectively handle peak workloads, reduce the impact of infrastructure failures, and support legacy system integration.

6. DISCUSSION

The results demonstrate that hybrid cloud systems function as essential elements for maintaining operational uptime while making hospital information systems accessible at all times. The study results show improved system availability, which enables healthcare organizations to maintain their operational activities, according to previous studies that demonstrate that hybrid systems that combine on-premises and cloud-based resources deliver both flexible system design and essential backup systems required in healthcare environments (Patel et al., 2021; Zhou et al., 2021).

Hospitals can use secure virtualized interfaces to connect their legacy biomedical devices because this solution allows them to keep their services active while using equipment that does not support current networking standards, which forms a major challenge for healthcare organizations that want to adopt digital transformation (Kumar et al., 2019; Alqahtani et al., 2021). The implementation of network segmentation, together with multilayered authentication systems, demonstrates that developers should create hybrid systems with security features as their primary design element. The segmentation system protects against lateral attacks because it restricts attackers from accessing multiple segments, which would enable them to reach essential patient information and hospital functions, supporting Singh and Chana's (2016) research on safe medical IoT deployments. The combination of optimized load balancing and containerized resource management systems results in decreased latency, which simultaneously enables hospitals to process unexpected increases in patient data without any operational interruptions (Sharma et al. 2020). This research adds to existing studies that promote healthcare organizations to implement hybrid cloud systems because the research proves that such systems can establish connections between outdated technology and modern systems that require continuous operation. The observed enhancements in operational effectiveness, security improvements, and increased data access demonstrate that hospitals that implement hybrid cloud systems obtain greater protection against both technical failures and cyber threats, which helps them maintain continuous patient care. Future research should investigate the long-term sustainability and cost-effectiveness of hybrid cloud solutions across hospitals of diverse sizes and geographies.

The implementation of a high-availability hybrid cloud architecture in hospital information systems demonstrates operational resilience and security improvement. Hospitals can enable continuous access to essential data and applications by combining cloud resources with their existing on-premises systems, which protects their operations from hardware failures and high-demand situations (Patel et al., 2021; Zhou et al., 2021). The implementation of secure network segmentation, together with virtualization technologies, enables organizations to use their existing biomedical devices while maintaining system security, which resolves the fundamental problems that medical IT professionals have faced since the beginning of their work (Kumar et al., 2019; Alqahtani et al., 2021). The study findings demonstrate that hybrid cloud implementation increases system availability while enabling organizations to perform load distribution and container resource management and implement security measures, all of which contribute to optimal healthcare performance (Sharma et al., 2020; Singh & Chana, 2016). The study results prove that hybrid cloud infrastructure systems work as essential technologies because they enable medical organizations to update their outdated systems without disrupting their current IT operations. Hybrid cloud solutions offer hospitals a valuable method for updating their data management systems because they enable medical institutions to operate their systems continuously with strong defense measures. This study needs to investigate how hospitals can use their resources efficiently and assess the long-term sustainability and technological compatibility of these systems across different hospital sizes and types. The implementation of high-availability hybrid cloud architectures creates a security measure that helps healthcare organizations deliver efficient and secure services to patients.

7. CONCLUSION

REFERENCES

Alharthi, A., Alfarhood, A., & Alsaadi (2022). Secure Data Protection Mechanisms For Hybrid Cloud Healthcare Environments. Ieee Access, 10, 56789–56803. Https://Doi.Org/10.1109/Access.2022.3165543

Alqahtani, F., Alghamdi, H., & Alshehri, M. (2021). Cloud-Based Healthcare Systems: Challenges and Opportunities For High Availability. Journal Of Healthcare Informatics Research, 5(2), 87–104. Https://Doi.Org/10.1007/S41666-021-00092-3

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Zaharia, M. (2010). A View of Cloud Computing. Communications Of the Acm, 53(4), 50–58. Https://Doi.Org/10.1145/1721654.1721672

Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. Ieee Transactions on Dependable and Secure Computing, 1(1), 11–33. Https://Doi.Org/10.1109/Tdsc.2004.2

Behl, A., & Behl, K. (2017). Cybersecurity And Cyberwar: What Everyone Needs to Know. Oxford University

Press. Https://Doi.Org/10.1093/Wentk/9780190258208.001.0001
Bhattacharya, S., & Roy, A. (2019). Workload Balancing and Fault Tolerance in Cloud-Enabled Hospital Systems. International Journal of Information Management, 45, 150–160. Https://Doi.Org/10.1016/J.Ijinfomgt.2018.11.012
Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration Of Cloud Computing and Internet of Things: A Survey. Future Generation Computer Systems, 56, 684–700. Https://Doi.Org/10.1016/J.Future.2015.09.021
Buyya, R., Calheiros, R. N., & Dastjerdi, A. V. (2016). Fog Computing and Its Role in the Internet of Things. Proceedings Of the Ieee, 104(1), 73–89. Https://Doi.Org/10.1109/Jproc.2015.2496061
Chen, M., Ma, Y., Li, Y., Wu, D., Zhang, Y., & Youn, C. H. (2017). Wearable 2.0: Enabling Human-Cloud Integration In Next-Generation Healthcare Systems. Ieee Communications Magazine, 55(1), 54–61. Https://Doi.Org/10.1109/Mcom.2017.1600397
Ghosh, R., & Naik, V. K. (2012). Biting Off Safely More Than You Can Chew: Predictive Analytics for Resource Over-Commit In Iaas Cloud. Ieee 5th International Conference on Cloud Computing, 25–32. Https://Doi.Org/10.1109/Cloud.2012.82
Hussein, M., & Ahmed, S. (2020). Cloud Orchestration Frameworks for Continuous Hospital Information System Availability. Journal Of Biomedical Informatics 107, 103470. Https://Doi.Org/10.1016/J.Jbi.2020.103470
Kuo, A. M. H. (2011). Opportunities And Challenges of Cloud Computing to Improve Healthcare Services. Journal Of Medical Internet Research, 13(3), E67. Https://Doi.Org/10.2196/Jmir.1867
Li, X., Wang, Y., & Chen, Z. (2021). High-Availability Healthcare Systems Using Hybrid Cloud Architectures. Computers In Industry, 128, 103421. Https://Doi.Org/10.1016/J.Compind.2021.103421
Marinos, A., & Briscoe, G. (2009). Community Cloud Computing. Cloud Computing, 472–484. Https://Doi.Org/10.1007/978-3-642-10665-1_43
Mell, P., & Grance, T. (2011). The Nist Definition Of Cloud Computing. Nist Special Publication, 800(145), 1–7. Https://Doi.Org/10.6028/Nist.Sp.800-145
Puthal, D., Ranjan, R., Nanda, A., & Zomaya, A. Y. (2018). Secure Authentication and Load Balancing of Distributed Cloud Data Centers. Ieee Transactions on Cloud Computing, 6(2), 403–416. Https://Doi.Org/10.1109/Tcc.2016.2556748
Rittinghouse, J. W., & Ransome, J. F. (2017). Cloud Computing: Implementation, Management, And Security. Crc Press. Https://Doi.Org/10.1201/9781315274756
Singh P., Kumar R. (2022). Secure Healthcare Systems Using Hybrid Cloud and Virtualization Technologies. Computers, Materials & Continua, 72(3), 5331–5347. Https://Doi.Org/10.32604/Cmc.2022.021654
Wang, J., Liu, H., & Zhang, L. (2021). A Hybrid Cloud-Based Hospital Information Management System with Enhanced Security and Reliability. Journal Of Medical Internet Research, 23(6), E25792. Https://Doi.Org/10.2196/25792
Zhang, Y., & Li, P. (2020). Reliable Cloud-Based Healthcare Systems With Legacy Medical Device Integration. Ieee Transactions on Cloud Computing, 8(4), 1056–1067. Https://Doi.Org/10.1109/Tcc.2019.2920441