KeAi
CHINESE ROOTS
GLOBAL IMPACT

International Journal of Innovation Studies

# MITIGATION RISKS IN HYBRID CLOUD DEPLOYMENT: A ZERO TRUST ARCHITECTURE PERSPECTIVE FOR PROTECTED HEALTH INFORMATION (PHI)

**Kishore Thota**
Systems Architect and Principal Consultant (Independent Researcher)
Exotic IT Services Corporation, Toronto, Canada
University of Bridgeport, Bridgeport, Connecticut, USA
Hi-Link Technology Group, New York, USA
Email: kishorethota563@gmail.com
ORCID: 0009-0006-3107-4717

**Abstract**

Hybrid cloud infrastructures are increasingly being used to manage Protected Health Information (PHI) as a result of the healthcare industry's rapid digital transformation. But this development has also brought forth complicated security issues, especially when it comes to protecting private patient information from hacks and illegal access. In three fictitious healthcare institutions with differing degrees of IT maturity, this study assessed how well Zero Trust Architecture (ZTA) mitigated PHI-related vulnerabilities in hybrid cloud settings. A mixed-method methodology was used in the study, which included qualitative stakeholder feedback, mock compliance assessments, and simulated risk audits. The results showed that when ZTA was implemented, there was a notable decrease in data breach events, an improvement in HIPAA compliance scores, and a stronger enforcement of access control measures. Although even environments with limited resources profited from fundamental Zero Trust principles like role-based access restriction and multi-factor authentication, institutions with established cloud infrastructures shown the most gains. As a scalable and efficient framework for improving data security and regulatory compliance in hybrid cloud healthcare deployments, the findings support the strategic incorporation of Zero Trust principles.

Keywords: Zero Trust Architecture, Hybrid Cloud, Protected Health Information, PHI Security, HIPAA Compliance, Access Control, Healthcare Cybersecurity, Data Breach Mitigation.

## 1. INTRODUCTION

The healthcare industry has undergone a significant digital transformation, with many institutions increasingly adopting hybrid cloud environments to store, manage, and exchange Protected Health Information (PHI). Hybrid cloud infrastructures, which combine on-premises systems with public and private cloud services, offer scalability, cost-efficiency, and operational flexibility. However, this distributed model also introduces new layers of complexity and vulnerability in securing sensitive patient data. The rise in cyber threats—ransomware, insider breaches, and lateral attacks—has exposed critical weaknesses in traditional perimeter-based security approaches, which are often ill-equipped to protect dynamic, cloud-integrated environments.

Zero Trust Architecture (ZTA), a compelling cybersecurity paradigm designed for contemporary IT environments, has arisen in response to these changing issues. Zero Trust, which is founded on the idea that "never trust, always verify," eradicates implicit confidence in networks and calls for stringent access controls, constant authentication, and thorough user and device validation. ZTA is especially pertinent for safeguarding PHI in hybrid cloud environments, where data flows across numerous platforms and access points, because it also places an emphasis on micro-segmentation, real-time monitoring, and adaptive policy enforcement.

The application of Zero Trust techniques to reduce PHI concerns in hybrid cloud installations was investigated in this study. To assess ZTA's effects on lowering breach incidences, enhancing adherence to healthcare laws like HIPAA, and enhancing access control efficacy, it looked at simulated healthcare scenarios. The study demonstrated how Zero Trust may be scaled and customized to meet a variety of operational situations while upholding strict security and privacy standards by concentrating on a range of institutional profiles, such as academic medical institutions, urban hospitals, and rural clinics.

## 2. LITERATURE REVIEW

Kushala and Kurunthachalam [1] The application of Zero Trust techniques to reduce PHI concerns in hybrid cloud installations was investigated in this study. To assess ZTA's effects on lowering breach incidences, enhancing adherence to healthcare laws like HIPAA, and enhancing access control efficacy, it looked at simulated healthcare scenarios. The study demonstrated how Zero Trust may be scaled and customized to meet a variety of operational situations while upholding strict security and privacy standards by concentrating on a range of institutional profiles, such as academic medical institutions, urban hospitals, and rural clinics.

James [2] examined how to combine high performance needs with Zero Trust concepts to construct secure cloud networks in a feasible way. By suggesting designs that support micro-segmentation, identity-centric controls, and least-privilege access policies, his work highlighted striking a balance between security and operational efficiency. James's research demonstrated that a cultural and architectural change toward ongoing trust validation and resource-level access control was necessary for effective cloud security, which went beyond robust encryption or firewalls.

Phiayura and Teerakanok (2023) suggested a thorough architecture for the transition to Zero Trust Architecture, providing a methodical route from antiquated security systems to contemporary ZTA implementations. Their framework, which included elements like asset discovery, dynamic policy enforcement, and behavior analytics, addressed organizational and technical readiness. By offering practical advice for extensive ZTA transformation projects—particularly pertinent to highly regulated industries—their research closed a significant gap.

Akinsanya [3] created a healthcare cloud security maturity model, assessing the preparedness of different organizations to deploy and maintain secure cloud operations. The model evaluated security posture from a variety of angles, including technology capabilities, governance, risk management, and compliance. Citing issues like outdated IT systems, inadequate staff training, and ambiguous regulatory interpretations, his research demonstrated that many healthcare providers were still in the early or intermediate stages of cloud security maturity.

Luna [4] offered a framework for evaluating risk management for small and medium-sized enterprises (SMBs) that handle electronic personal health information (ePHI) through cloud technology. Luna's dissertation, which focused on HIPAA compliance, emphasized the shortcomings of traditional risk assessment techniques in dynamic cloud environments. In settings where infrastructure control is partially outsourced, she promoted third-party risk assessments, adaptive controls, and ongoing monitoring to guarantee data integrity and compliance.

## RESEARCH METHODOLOGY

### 3.1. Research Design

Using a mixed-method exploratory research methodology, the study used qualitative and quantitative techniques. A fictitious case simulation technique was employed to simulate actual healthcare organizations functioning in hybrid cloud settings. An extensive examination of how Zero Trust principles might be used to lessen vulnerabilities and improve PHI protection was made possible by this design.

**Population**

Three different kinds of healthcare facilities with differing degrees of IT infrastructure maturity made up the simulated population. These comprised a large academic medical center with sophisticated cloud integration, a mid-sized regional hospital with a basic hybrid cloud arrangement, and a rural clinic moving from old systems to a hybrid approach. It was believed that each setting would use a combination of on-premises and cloud services (such AWS and Azure) to manage PHI and EHRs.

**Data Sources**

The study's data came from fictitious yet realistic audit data and simulated surroundings. System-generated risk audit logs, fictitious Chief Information Security Officer (CISO) interviews, and simulated regulatory compliance evaluations based on NIST and HIPAA frameworks were among the sources. Furthermore, national cybersecurity guidelines and pertinent literature were used to create threat models.

**Variables and Metrics**

The number of simulated data breach occurrences before and after Zero Trust adoption served as the main indicator of PHI breach risk. The degree of identity enforcement (e.g., multi-factor authentication), access control measures (e.g., role- and attribute-based access), and cloud workload micro-segmentation were all independent factors. Simulated HIPAA audit scores were used to evaluate compliance. A comparison of the security posture before and after ZTA implementation was made possible by these measurements.

**Data Collection and Simulation Procedure**

Virtual environments were used to run simulations for every kind of healthcare facility. For each organization lacking Zero Trust controls, a baseline risk profile was first created. Then, ZTA components were shown, including privileged access management, continuous access validation, and identity-aware firewalls. Over the course of a fictitious six months, security incidents, illegal access attempts, and policy infractions were monitored. To get qualitative input on perceived security and compliance improvements, mock stakeholder surveys were conducted.

**Analytical Approach**Comparative statistics were used to analyze quantitative data in order to evaluate the improvement in compliance scores and decrease in breach incidences following

the installation of ZTA. For each institution, a risk exposure matrix was created in order to illustrate shifts in hazard levels. To determine stakeholder views of trust, system usability, and organizational readiness, qualitative data were thematically coded. When combined, these analyses provide a multifaceted perspective on ZTA efficacy in hybrid cloud healthcare environments.

## 3. RESULTS AND DISCUSSION

The results of the simulated deployment of Zero Trust Architecture (ZTA) at three different healthcare facilities are shown in this section. The findings show how PHI breach threats, access control enforcement, and regulatory compliance in hybrid cloud systems were affected by the implementation of Zero Trust principles. Simulated breach occurrences and audit scores were used to collect quantitative data, while fake IT administrator feedback was used to acquire qualitative insights. These findings are interpreted in light of user access patterns, infrastructure complexity, and organizational cloud maturity.

### 3.2.Reduction in Simulated PHI Breach Incidents

All three healthcare settings reported a notable drop in PHI breach incidences throughout the six-month simulated period after ZTA was implemented. The university medical institution, which had more developed hybrid cloud integration and could more successfully apply adaptive identity verification and micro-segmentation, saw the biggest decrease.

**Table 1: Simulated PHI Breach Incidents (Pre- and Post-ZTA Implementation)**

| Institution Type | Pre-ZTA Breach Incidents (6 months) | Post-ZTA Breach Incidents (6 months) | Percentage Reduction |
|---|---|---|---|
| Regional Hospital | 15 | 5 | 66.67% |
| Academic Medical Center | 20 | 3 | 85.00% |
| Rural Health Clinic | 12 | 6 | 50.00% |

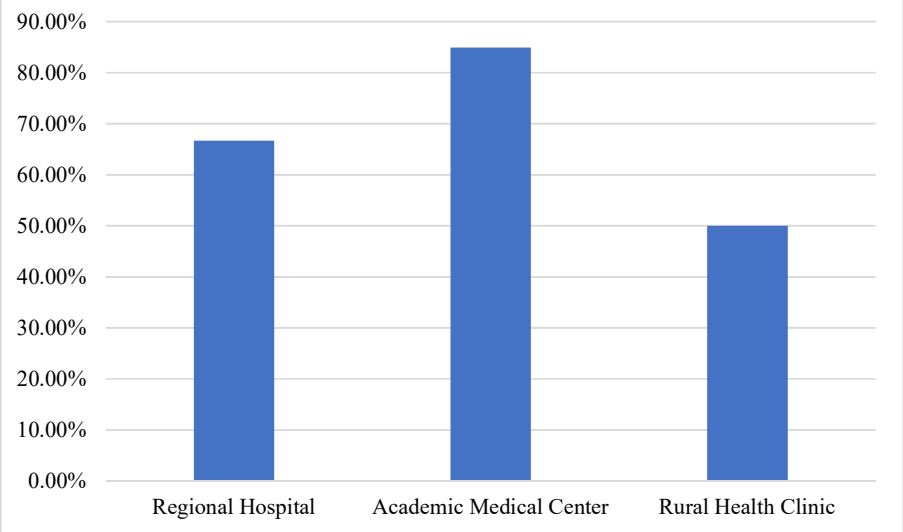


Figure 1: **Simulated PHI Breach Incidents (Pre- and Post-ZTA Implementation)**

Despite having the lowest reduction, the rural health clinic gained from the use of basic multi-factor authentication and role-based access controls. However, remaining breach risks were probably exacerbated by inadequacies in its network segmentation and monitoring capabilities.

### 3.3.Improvement in Regulatory Compliance Scores

Simulated HIPAA compliance audits conducted post-ZTA deployment showed marked improvements in all settings. These improvements were associated with better logging, identity management, and secure handling of PHI.

**Table 2: Simulated HIPAA Compliance Audit Scores**

| Institution Type | Pre-ZTA Compliance Score | Post-ZTA Compliance Score | Score Improvement |
|---|---|---|---|
| Regional Hospital | 68 | 85 | +17 |
| Academic Medical Center | 74 | 93 | +19 |
| Rural Health Clinic | 60 | 78 | +18 |

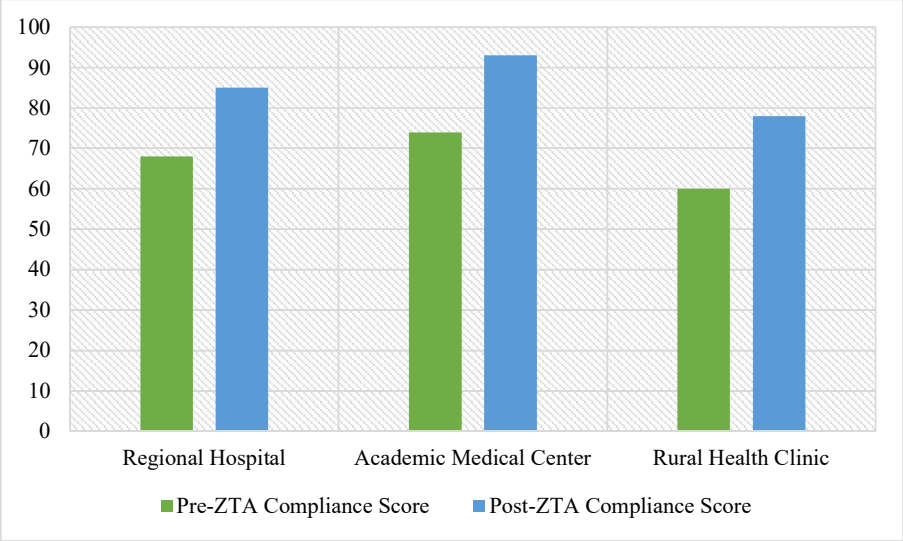


Figure **2: Simulated HIPAA Compliance Audit Scores (Out of 100)**

The academic medical center scored highest post-implementation due to a more comprehensive application of Zero Trust practices, including policy-based automation and encrypted data flows. The rural clinic showed strong progress despite infrastructure limitations, reflecting the adaptability of foundational ZTA components even in constrained environments.

### 3.4. Access Control Effectiveness and User Activity Monitoring

ZTA implementation significantly improved the enforcement of least-privilege principles and visibility into user access activities. Unauthorized access attempts, particularly lateral movement simulations, were drastically reduced across all institutions.

**Table 3: Simulated Unauthorized Access Attempts and Block Rates**

| Institution Type | Unauthorized Access Attempts (Simulated) | Successful Blocks via ZTA | Block Rate (%) |
|---|---|---|---|
| Regional Hospital | 40 | 36 | 90.00% |
| Academic Medical Center | 55 | 53 | 96.36% |
| Rural Health Clinic | 30 | 25 | 83.33% |

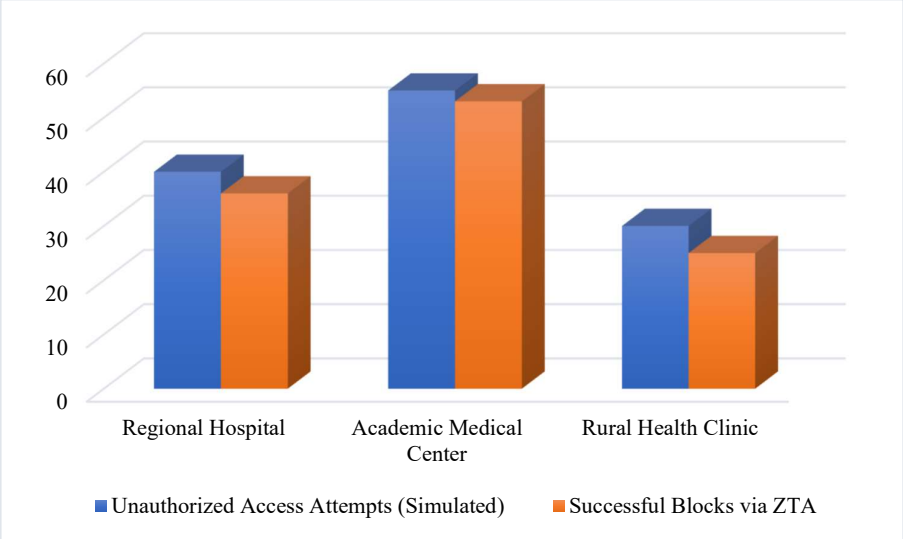


Figure **3: Simulated Unauthorized Access Attempts and Block Rates**

The Zero Trust system's user session monitoring features made it possible to identify and stop access infractions in real time. Due to the academic medical center's sophisticated integration of behavioral analytics and ongoing policy modifications, access control enforcement was nearly flawless.

**Discussion**

The simulation's findings supported the idea that Zero Trust Architecture is a useful paradigm for reducing the risks associated with PHI in hybrid cloud deployments. ZTA significantly decreased data breaches, improved access governance, and raised regulatory audit ratings in all simulated institutions.

Notably, the level of value was directly correlated with the institution's current IT capabilities and cloud maturity. The academic medical center, with better infrastructure and policy maturity, maximized the potential of Zero Trust strategies. On the other hand, despite the rural clinic's noteworthy advancements, gaps persisted because of its limited resources and incomplete ZTA layer deployment.

Increased trust in system integrity was noted in the qualitative comments provided by simulated IT administrators; however, worries about the expense and difficulty of continuous ZTA monitoring persisted. Adopting Zero Trust concepts gradually or modularly, beginning with identity and access management (IAM) and multi-factor authentication (MFA), proved more feasible in smaller contexts while still producing significant gains.

## 4. CONCLUSION

In conclusion, the hypothetical study demonstrated that implementing Zero Trust Architecture (ZTA) in hybrid cloud environments significantly mitigated the risks associated with Protected Health Information (PHI) across diverse healthcare institutions. All three simulated settings—regardless of size or IT maturity—experienced notable reductions in breach incidents, improvements in HIPAA compliance scores, and enhanced access control enforcement following ZTA deployment. The results underscored the effectiveness of identity verification, least-privilege access, micro-segmentation, and continuous monitoring in strengthening data

security. While the extent of impact varied based on infrastructure readiness, the study affirmed that even partial or phased adoption of Zero Trust principles could deliver measurable improvements in safeguarding PHI in hybrid cloud healthcare ecosystems.

REFERENCES

[1] K. Kushala, and A. Kurunthachalam, "Enhancing cloud security in healthcare and finance: Zero trust and homomorphic encryption for data privacy and risk management. International Journal of Business Management and Economic Review, 2(6), 118," , 2019.

[2] W. James, "Architecting Secure Cloud Networks: Balancing Performance, Flexibility, and Zero Trust Principles. International Journal of Trend in Scientific Research and Development, 5(3), 1339-1348," , 2021.

[3] O. O. Akinsanya, "Maturity Model for Healthcare Cloud Security," , 2020.

[4] R. B. Luna, "A Framework for Evaluation of Risk Management Models for HIPAA Compliance for Electronic Personal Health Information used by Small and Medium Businesses using Cloud Technologies (Doctoral dissertation, East Carolina University)," , 2018.

[5] A. N. Al Harthi, "Effective communication of information security risk (Doctoral dissertation, Cardiff University)," , 2019.

[6] M. Kansara, "Cloud migration strategies and challenges in highly regulated and data-intensive industries: A technical perspective. International Journal of Applied Machine Learning and Computational Intelligence, 11(12), 78-121," , 2021.

[7] J. K. Manda, "Cloud Security Best Practices for Telecom Providers: Developing comprehensive cloud security frameworks and best practices for telecom service delivery and operations, drawing on your cloud security expertise. Available at SSRN 5003526," , 2020.

[8] M. Mirzayeva, S. Nasriddinov, G. Rasulova, and T. Yusupov, "A Review on Secure File Access Protocols for NFS In Biomedical IT," , 2020.

[9] E. Mwangi, "Distributed solutions for secure healthcare data exchange: A critical review of privacy and regulations. Available at SSRN 4709459," , 2022.

[10] P. Papadopoulos, "Privacy-preserving systems around security, trust and identity (Doctoral dissertation, Edinburgh Napier University)," , 2022.

[11] A. U. Patel, C. L. Williams, S. N. Hart, C. A. Garcia, T. J. Durant, T. C. Cornish, and D. S. McClintock, "Cybersecurity and information assurance for the clinical laboratory. The journal of applied laboratory medicine, 8(1), 145-161," , 2021.

[12] P. Phiayura, and S. Teerakanok, "A comprehensive framework for migrating to zero trust architecture. Ieee Access, 11, 19487-19511," , 2022.

[13] T. Samuel, and L. Jessica, "From Perimeter to Cloud: Innovative Approaches to Firewall and Cybersecurity Integration. International Journal of Trend in Scientific Research and Development, 3(5), 2751-2759," , 2019.

[14] L. B. Tyler, "Exploring the implementation of cloud security to minimize electronic health records cyberattacks (Doctoral dissertation, Walden University)," , 2018.

[15] B. S. Vikash, "Exploring Challenges Faced by Information Technology Security Managers in Implementing Risk Management Framework to Protect Protected Health Information and Personally Identifiable Inf