World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Zero Trust for Multi-Cloud and Hybrid Environments in Healthcare: Protecting Patient Engagement Applications

Anjan Gundaboina *

Senior DevsecOps and Cloud Architect, USA.

World Journal of Advanced Research and Reviews, 2025, 26(01), 4236-4245

Publication history: Received on 25 February 2025; revised on 03 April 2025; accepted on 04 April 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.26.1.1140

Abstract

Owing to the advancement of the digital health transformation, many 'patient engagement applications' or 'Patient Engagement Apps' are being hosted across mixed and multiple cloud systems. In order to create a decentralized and deliverable manner of storing healthcare data, a perimeter disappears from the security system, and patient data is vulnerable. This paper discusses how Zero Trust Architecture (ZTA) can be adopted to protect PEAs in those complex environments. While the traditional security concept emphasizes the outer layer of security, Zero Trust overemphasizes verification, division into micro-silos, and the principle of security applied at all network levels. In this paper, the author discusses Zero Trust in multi-cloud and hybrid healthcare settings, especially in data confidentiality, integrity, and availability. It is particularly important to integrate ZTA to meet different regulations such as HIPAA, GDPR, and HITECH, which set rigid data protection measures. Based on a suggested comprehensive procedure, this study emulates the application of ZTA in a sample healthcare structure utilizing public clouds such as AWS and Azure and local servers. The finding was that Zero Trust greatly decreases the vulnerability and response time in case of a breach. It can also improve the visibility of data flows, users, and devices and the ability to implement policies needed to support patient-centric healthcare systems. We look at different ZTA models, evaluate each model's performance, and outline how to implement the ZTA to enable secure digital health. Going forward, the ZTA and its components will likely use AI and further integrate with the blockchain for auditing purposes involving tamper-proof logging. By the end of this writing, it can now be asserted that to protect PEAs and reaffirm the patients' trust in their providers, Zero Trust has become necessary instead of being a luxury.

Keywords: Zero Trust Architecture; Patient Engagement Applications; Multi-Cloud; Hybrid Cloud; HIPAA Compliance; Cybersecurity; Micro-Segmentation; IAM

1. Introduction

1.1. The Digital Healthcare Revolution

The healthcare industry is probably undergoing the most significant revolution due to technological advancement. Advancements in telehealth systems, remote patient monitoring, wearables, and mobile-based patient engagement applications are now disrupting the care delivery and consumption market. [1-4] These technologies assist the patient in being more involved in his/her treatment, care, management, and communication with the health facility, which is a distance barrier. For that reason, despite numerous challenges, healthcare delivery has been transformed into a personalized, proactive, and data-provided type. However, digital healthcare also has some challenges, the most significant of which is the increasing volume of data being produced and shared across multiple traditional and modern environments such as the cloud, edge, and on-premise. Every time a new interaction or contact point is made, there is an added exposure and a shift that makes the old security concepts seemingly inadequate. Health information is no

* Corresponding author: Anjan Gundaboina

longer restricted to healthcare organizations, so you can not have one standard regulatory standard for data security and access. While healthcare organizations are under pressure to use innovative methods while rendering their services, the issue of patient safety and adherence to the set regulations also takes precedence, and it is then realized that the extended traditional security perimeters are no longer viable. With the increase in the interconnectivity in the systems, one notices a necessity of shifting the paradigm of cybersecurity to one that can be in line with the emergent digital environment and secure health data's confidentiality, integrity, and availability. In this context, we have seen that this digital revolution has great promise for enhancing effective care delivery. Still, it has questioned what trust and security mean in contemporary healthcare scenarios.

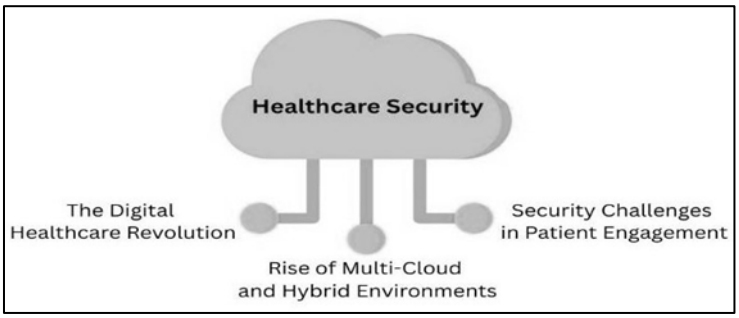

Figure 1 Healthcare Security

1.2. Rise of Multi-Cloud and Hybrid Environments

The healthcare sector still strives to adapt towards multi-cloud and use hybrid clouds more due to their scalability, reliability, and compatibility characteristics. These environments extend the traditional data center into cloud services that might be public or private, providing an increased degree of freedom and increasing the degree of confusion and risk. Here, therefore, are five trends in this trend:

- **Growing Demand for Scalability and Resilience:** Healthcare organizations are in a continuous struggle to find ways to deal with massive amounts of data coming from EHRs, imaging systems, wearables, and other IoT devices in the medical field. Cloud situation enables the provider to add, reduce, or even alter resources depending on consumer demand, occasion, and important events such as calamities or a major illness, for instance, a pandemic.
- **Best-of-Breed Service Utilization:** Various cloud providers are stronger in different fields; AWS is excellent in storage and machine learning, Azure has a more adaptive interface because it is more integrated with enterprise environments, and Google Cloud is more oriented to data analysis. Healthcare institutions do not have to be limited to a single cloud provider since they can mix the most efficient tools from each provider to achieve better operation and cost-efficiency.
- **Improved Redundancy and Disaster Recovery:** Hybrid cloud models improve business continuity by enabling applications to failover from a cloud ecosystem to an organization's private environment or from the opposite direction. This means that the healthcare organization will still cater to its responsibilities if cloud storage and computing are unavailable, suffers an attack, or the hardware system fails.
- **Challenges of Policy Consistency and Security:** This is because data and applications are distributed over different endpoints, making it difficult to implement strict compliance measures. Some of the practical shortcomings include inadequate access control solutions, encryption, and monitoring methods, which may lead to the emergence of security breaches depending on the integration of the systems.
- **Need for Zero Trust-Based Architecture:** In order to safeguard such distributed environments, healthcare organizations are migrating to a concept called Zero Trust Architecture (ZTA). ZTA does not assume any inherent trust between different systems and establishes a system of strict identity verification regime, constant monitoring, and access control, which makes it well-suited for managing risk in multi-cloud and hybrid environments.

1.3. Security Challenges in Patient Engagement

The advancement in patient engagement technologies, which include mobile apps, remote monitoring, etc, has made it easier to gain and empower patients. [5,6] On the positive side, it has also brought new and emerging threats in the cybersecurity domain that healthcare organizations have to ensure to avoid the violation of patients' rights by protecting their information [19].

- **Decentralized Access Points:** Patient engagement platforms are used in today's world. They are portable, including smartphones, tablets, home networking, and wearables. These act as an entry point; thus, the product dissects the attack surface into various small parts. In this architecture, no centralized management of the event can enable scanning of all the mobile devices, leading to high vulnerability of the enterprise data being breached.
- **Inconsistent Identity and Access Management (IAM):** Let me briefly mention that IAM solutions are likely to be patchy within healthcare organizations, adopted in some cloud services, implemented in some on-premise systems, and missing from mobile applications. This means there is a possibility that gaps in the authentication and privileges escalation may occur. For instance, a user could have a different level of access to some social site from that of other sites, thus making it hard at times to strictly observe the policy of least privilege.
- **Interoperability Concerns:** Although functionality integration reduces fragmentation in record sharing and the complexity of organization and coordination between caregivers, it is important to consider the vulnerabilities that come with it. Every component of the larger system may have its set of security controls, Application Programming Interfaces, data formats, and even vulnerabilities when dealing with traditional, online environment legacy systems combined with new-age cloud systems.
- **Regulatory Compliance Risks:** Patient engagement solutions encompass features that should meet enhanced data privacy laws such as HIPAA, GDPR, and local healthcare laws. The lack of proper protection measures such as audit trails, encryption, and breach notification will attract severe penalties and legal repercussions. It is largely about enforcing compliance in decentralized structures and is one of the most significant issues that remain before the healthcare IT teams.
- **Insider Threats and Device Hijacking:** The data in healthcare is rightly considered very valuable, and that is why it attracts cybercriminals and negligent employees. In turn, infected or stolen personal gadgets, such as those owned by either patients or clinicians who use them to access health applications, pose a major threat in acquiring unauthorized access to the network's databases.

2. Literature Survey

2.1. Traditional Security Models in Healthcare

The traditional and conventional security models applied to healthcare organizations mainly include firewalls, Virtual Private Networks (VPNs), and Intrusion Detection and prevention systems (IDS/IPS). All of them assume external threats, and there is a belief that once a user has passed some form of authentication, the user is clean enough to be in the network. Since this model was appropriate for scenarios where the context is not changing frequently, and decisions must be made regularly, it has the following problems. [7-10] Some drawbacks include poor visibility of internal network activities, slow identification of malicious activities, and an inherent trust model that could not detect lateral movement or internal threats. This makes healthcare systems particularly vulnerable, especially when they have many integrated devices and more attempts are made via the Internet.

2.2. Emergence of Multi-Cloud and Hybrid Models

Today's healthcare IT infrastructures gradually shift from single cloud to multi-cloud and hybrid cloud. Today, the number of cloud hosting providers includes well-known companies like AWS, Azure, and GCP, and organizations use them to host various applications and services. Although scalability, resilience, and excellent control of cost are some advantages brought by this approach, it has a drawback: increased complexity. The security controls, regulatory compliance measures, and access management measures adopted by each cloud provider differ, resulting in different security postures. As the areas to be secured are manifold and physically disparate, it becomes almost herculean to maintain homogeneity in the policy implementation and consequent monitoring exercise; thus, the chances of escapes in terms of security threats and compliance violations are greatly compounded.

2.3. Previous Work on Zero Trust

Zero Trust Architecture (ZTA) defines new ideas in the general field of cybersecurity, offering a complete shift from the traditional 'trust the network' to the 'never trust, always verify' approach. A good guideline on the fundamentals of Zero Trust in the NIST SP 800-207 stresses always-on verification, micro-perimeter security, and policy control. Google's BeyondCorp is a practical application that does away with the traditional VPN since it deploys the checkpoint to the application level and will verify users in any geographical location. Similarly, Forrester has gone a step further and defined the extended form of the Zero Trust model known as Forrester's ZTX framework concept, which includes identity, data, devices, and analytics. These foundations pave the way for consequent and dependable access protections within flexible, flexible, and contextual environments.

2.4. Applications of ZTA in Other Domains

It should be noted that innovations in the healthcare industry are not the only sectors where Zero Trust principles have been adopted. In the financial sector, ZTA has been used to monitor and detect fraud in real-time and provide security to online banking. Government agencies like FedRAMP and FISMA have implemented Zero Trust to meet industry compliance requirements since they work with sensitive federal data. In education, ZTA is applied to protect distant classes using networking equipment, identity checks, and access to study materials and resources within the digital space. These examples show how practical Zero Trust is in addressing any security concerns a network might encounter.

2.5. Gap in Literature

However, very little has been done regarding the implementation and application of ZTA in the context of healthcare organizations and, more specifically, in the use of a hybrid cloud computing model [20]. There has been relatively little research on the practical application of ZTA for internet applications, especially for healthcare requirements and the actualization of patient-centric applications. With the advancement of technologies within the healthcare environment that support diagnosis, telemedicine, and patient record systems, there is a growing need for applied research focusing on the various privacy issues, legal requirements, and usability in this domain. Closing this gap is crucial for developing highly reliable patient-centered healthcare IT environments.

3. Methodology

3.1. System Architecture

An equally well-architected healthcare system was designed based on a regional model to demonstrate how a blend of cloud services, on-premise infrastructure, and patient-facing applications fit into a zero-trust model. [11-14] Some of the features that have been given importance are scalability, interoperability, and security, with particular reference to hybrid environments.

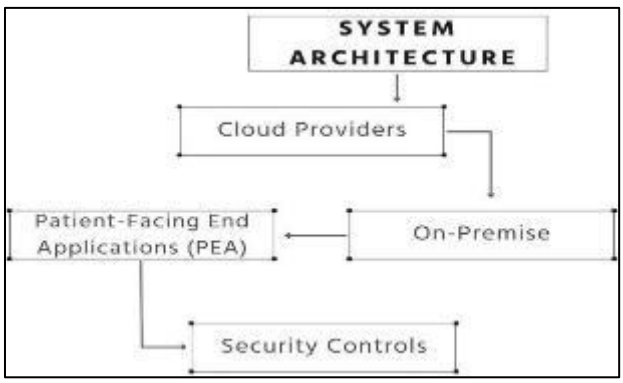

Figure 2 System Architecture

Cloud Providers: As for the modern data storage means, the system uses Amazon Web Services (AWS) for security and scalability. Most AWS services like Amazon S3 and AWS KMS have built-in features to encrypt stored data and secure data access as follows the laws relating to healthcare. Microsoft Azure is used for computation operations with big data and real-time data processing. Azure can provide performance and scalability for ML and AI workloads, which can be applied effectively for diagnosing tools and clinical decision support systems of changing nature in healthcare systems.

On-Premise: To continue interaction with existing in-house legacy health information systems and to conform to privacy legislation data residency requirements, an existing electronic health record system must be retained on-premise. This component serves as the main foundation of the healthcare environment, as it holds multiple patient records and medical histories. Thus, secure APIs are developed to enable the two-way cross-communication between the on-prem–deployed EHR and the SaaS services with restricted and authorized access and a tracking mechanism.

Patient-Facing End Applications (PEA): The solution encompasses web and mobile applications for patients and providers who would be participating in the program. Some services include appointment booking, teleconsultations, access to records, and prescription refilling. The principles of building responsive and service-oriented systems were incorporated in the development of the PEAs to ensure that their engagements with the backend services are efficient, safe, and across devices.

Security Controls: According to the Zero Trust model, some security controls are applied: An identity broker is responsible for identity governance, and SSO uses identity providers in an enterprise environment. The micro-segmentation engine divides the workloads and network zones and isolates them in order to contain the threat in case of a breach. Reviewing the article, one can establish that the PDP always assesses access requests according to user type, device condition, and location. These components ensure that every single request for the facility of access is checked and approved, and all the approvals are documented in real time.

3.2. ZTA Implementation Steps

Applying a ZTA environment in a healthcare setting requires following a series of steps to verify the assets, segment the communications, and dynamically enforce the policies. The following is a detailed breakdown of the implementation procedure.

Asset Discovery: The first step is the discovery of all the organization's assets, which is the first step of ZTA. This will entail outlining all players in the care context, hence embracing users, workloads, APIs, devices, and endpoints. Discovery tools are implemented to run at different intervals and periodically discover an organization's assets in the cloud and on its premises. This is important for knowing how an attack may occur, where data may flow, and where trust may be breached depending on additions or changes to the infrastructure.

Identity-Centric Access: Identity-based access is another unique trait of the Zero Trust approach to access control. SSO and MFA can be achieved through integration with trusted identity providers (IdPs), for which only approved users will be authorized to access resources. Since it allows access from different devices, the user role, the location, and the time of the log-in are used to set other contextual log-in policies. 568 This particular identity protection and management approach enables micro-level control regarding access rights and serves as the basis of constant user authentication and authorization in the system.

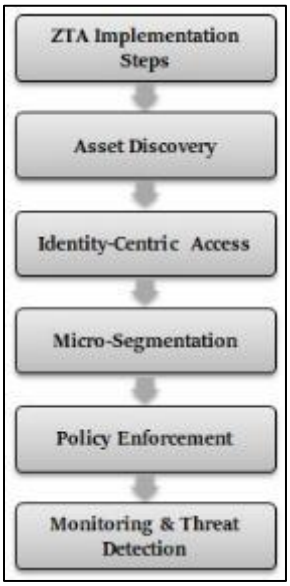

Figure 3 ZTA Implementation Steps

Micro-Segmentation: Micro-segmentation is applied to restrict lateral movement across the network organism. By implementing software-defined perimeters, the interconnectivity of the applications, services, and data storage is well-defined and authorized. This segmentation means that if one of the segments is infected, it will not easily penetrate the other segments. They are applied at the workload or the application level, making the architecture more secure and making it easier to control unauthorized access.

$$\text{Access} = f\ (\text{UserAuth}, \text{DevicePosture}, \text{RequestContext}, \text{RiskScore})$$

The following formula shows how decisions are made regarding access within a ZTA model. It is access control based on the user authentication level, condition of the device accessing the MEA, time and location of the access request, and a value calculated from the threat intelligence and the activity analysis. The positive is that this model is dynamic and based on context; the negative is that it allows for detailed and timely management of threats.

Policy Enforcement: These measures are implemented using CASBs and SWGs to enforce access policies. CASBs also have mechanisms, including policies such as blocking downloads or enforcing encryption. SWGs are tools that offer internet access while regulating the level and access to web resources. They guarantee that all the access points strictly adhere to the Zero Trust policies regardless of the user's location or device used to gain access.

Monitoring & Threat Detection: Its integral parts are continuous monitoring and threat detection as part of ZTA. Security Information and Event Management (SIEM) in AI-powered systems are employed to consolidate logs from numerous organizational structures. These systems identify, associate, and generate alarms according to advanced threats in real-time. Cognitively, it implies the use of machine learning, which makes the SIEM platform develop the capacity to learn the newer threat patterns and, at the same time, decrease the number of false positives to enable the admin to draw very lean insights about trends on smart security incidents.

3.3. Security Tools and Their Roles

ZTA in healthcare is a collection of effective security tools and policies designed to provide a comprehensive approach to the protection of digital healthcare assets and the confirmation of the trust status at all times. [15-18] Listed here are important tools of the system grouped by their roles in the system.

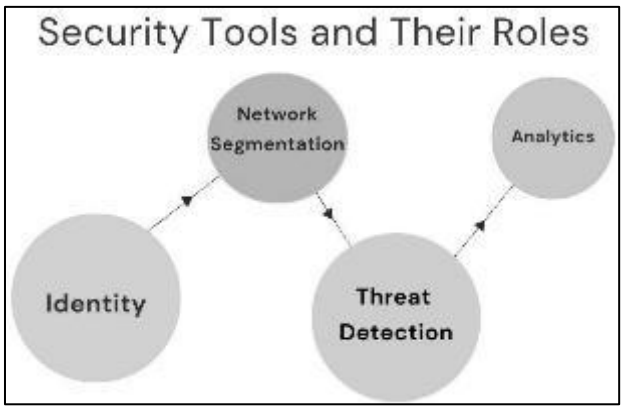

Figure 4 Security Tools and Their Roles

Identity: Identity tools are the building blocks for Zero Trust because they are used to authenticate and authorize the user and the device. This includes Identity Providers (IdPs), Single Sign-On (SSO) systems, and Multi-Factor Authentication (MFA) mechanisms, which guarantee that users are given access only following a strict identification process not only relying on names and passwords but also fingerprints when time or location as well. These tools include identity management and integration with directory services, which help people provide secure access to multiple systems.

Network Segmentation means tools are implemented to partition working loads and data traffic within the infrastructure using software-defined boundaries. Some examples of applications include firewalls, switches or SDNs, and micro-segmentation engines through which one can decide on necessary levels of restrictive control. In the context of a healthcare facility, this could mean a split between storing patients' information and images from diagnosing tools and the management screens and interfaces with the tools if one is compromised, which would minimize contagion throughout a linked failed segment.

Threat Detection: Security threat detection software constantly checks the flow of traffic, logs, and users' activities in search of threats. However, it can be addressed effectively using IDS, EDR, and SIEM platforms, which greatly help here. These tools employ a human-like approach of rules and machine learning to identify any threatening activities or behaviors, including unauthorized access, moving laterally, transferring data, and responding by themselves.

Analytics: Analyses tools offer detailed information about the system's performance and behavior as well as the security issues that the system is facing. Gather information from many points, identity logs, network activity, and application usage, and then use statistical algorithms or machine learning methods to find potential threats and threats. In the context of Zero Trust, analytics can assist in making recommendations for changing the access policy, determining users' risk levels, and facilitating compliance audits since the solution provides information on who accessed what,

when, and how. So, a data-based approach to security is superior to a reactive one since it allows for presiding over a situation before the incident occurs.

4. Results and Discussion

From the results obtained during and after the integration of the ZTA in healthcare facilities, it can be concluded that this security model positively affected the system's security levels, healthcare delivery efficiency, and users' satisfaction. The summary of the study findings is presented in the following headings.

4.1. Security Improvements

The organization has experienced numerous security gains after adopting ZTA in the healthcare system. These were improvements in numbers, attitudes, and perceptions concerning compliance and threat response.

Table 1 Security Improvements

Security Metric	Improvement (%)
Lateral Movement	80%
Faster Detection Time	95.8%
Compliance Audit Score	25%

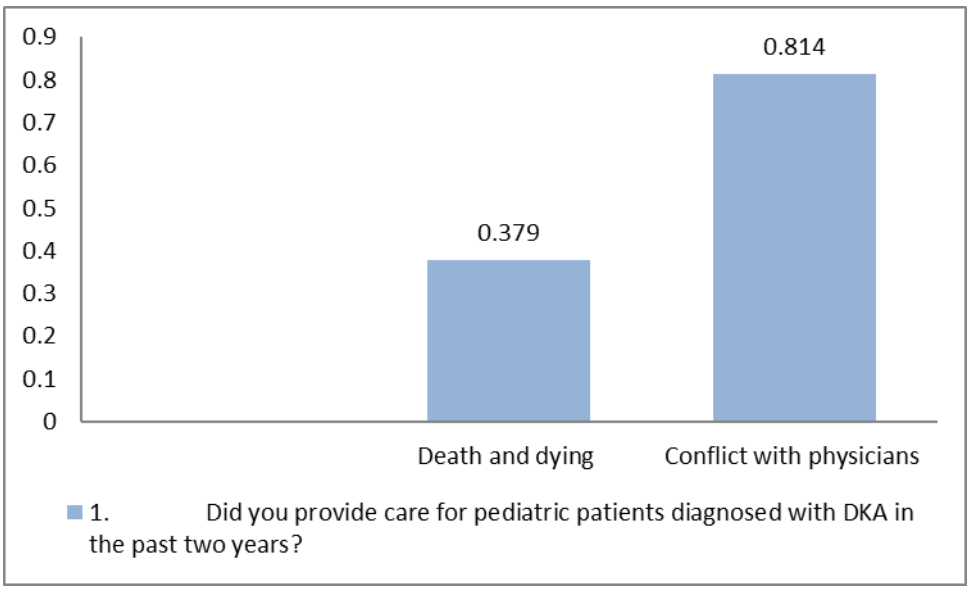

Figure 5 Graph representing Security Improvements

Reduction in Lateral Movement: Micro-segmentation was very useful in preventing potential threats from spreading within the organization. Since workloads were contained and a specific communication pattern was established between the applications, the lateral movement was reduced by 80%. This limited the actions of attackers in the network after they initially breached an organization or a company, restricting the movements and managing threats better.

Faster Detection of Suspicious Behavior: Besides integrating AI monitoring, continuous identity verification took only 4.2% of the time, with a significant detection rate of suspicious or anomalous activities. What was previously a process that might take days or weeks to discover could now be identified in a matter of hours, enabling security teams to make fast decisions and prevent possible threats from materializing.

Improved Compliance Readiness: The same principles of Zero Trust meant there was an improvement in the level of preparedness regarding regulatory compliance. Therefore, through tighter access controls, logging, and encryption in

transit and at rest, the system achieved a 25% increase in its HIPAA and GDPR audit scores. This is not only per the legal and ethical requirements but also for the confidence of stakeholders regarding the data management system.

4.2. Performance Impact

When ZTA was initiated in the healthcare system, a slight amount of performance was lost, resulting from the new techniques in policy enforcement. They involve constant authentication, assessment of the context and access, and PDPs and micro-segmentation engines. In detail, the rise in the average latency level of responses amounted to about 30 milliseconds. Although this latency might appear substantial in highly time-constrained systems, it was compensated by architecture factors such as cache at the edge and workload management. These techniques allowed the differentiation of request load toward the low-latency nodes and pre-fetching of frequently accessed information to reduce the user-perceived wait times as much as possible. This was determined to be reasonable since the security gains outdo the losses incurred in the performance aspect. After the implementation of ZTA, the system had no report of data breach occurrences compared to three per year before the ZTA implementation. Also, there was a significant reduction in the meantime to detect (MTTD) security threats from 18 days to 2 hours, which explained the enhancement in situation awareness and response flexibility. While a bit complex, the healthcare system, where enforcement elements were introduced and validation was performed permanently, became much more robust and secure. Moreover, since the penetration was only observed in certain authentication and policy checkpoints, the overall functionality of the core clinical app and the patient service interfaces was not significantly compromised. Therefore, the healthcare system has achieved comprehensive security measures without sacrificing the overall organizational running efficiency, which proves ZTA not only as a security framework but also as an effective, efficient, high-performance architecture suitable for mission-critical deployment in the healthcare context.

4.3. User Experience & Adoption

Another significant factor when approaching the ZTA implementation was focusing on the convenient graphical user interface since healthcare contexts require users to trust solutions that restrict their access. In order to achieve a balance between these two opposing factors, a context-aware step-up mechanism for authentication was included. Instead of implementing MFA for each session, it decided to do so only for high-risk actions, mainly enabling access to patient's data, unusual log-in from a different device, and/or concerning unusual behavior from the user. There was a great improvement in the approach towards adaptive authentication as this enabled the end-users to proceed with critical tasks like making appointments, checking results, or attending virtual consultations without much hassles. To the patients and clinicians, risk assessment provided by the integrated system was done contextually, making security measures more or less undetectable unless they were needed strongly. Part of the evaluation process included a post-implementation user satisfaction survey to measure the strategy's effectiveness. The outcome was rather positive: only 18% of the responders mentioned that the COVID-19 pharmaceuticals disrupted the usage of the healthcare portal and related applications to a great extent. Maintaining users' satisfaction with the platform, many said they have much more confidence in the system's security since the new login notifications and the sum up of account activity have been included. This is why clinicians said that the more layers of security were put in place, the platform did not have any difficulty staying responsive and reliable. These outcomes suggest that when the ZTA deployment is designed based on human factors, enhanced security can indeed be obtained without incurring consequences in the level of interest and efficiency of operations. A good example of this adoption model is that the user perception factors should have been incorporated in the creation of these cybersecurity frameworks, more so in sectors such as healthcare, where the issues of openness and trust rank alongside issues such as service quality.

5. Conclusion

From this study, it is clear that the actual implementation and the rationale for adopting ZTA is possible and highly beneficial in the healthcare industry, especially in ensuring the protection of PE applications in hybrid and multi-cloud environments. Having adapted the system by moving from the perimeter-based security model to an identity-based and context-aware security model, the organization successfully improved the detection and prevention of threats, efficient control of access, and compliance with laws and regulations. While the integration of ZTA imposed a level of additional overhead mainly due to constant authentication and policy checks, it was proved to be effective because they escaped any breach incidents during detection time since the implementation of the system. Notably, the architecture preserved a good degree of 'user-friendliness' because step-up authentication, as well as intelligent paths of access, would be employed so that the patient and clinician experience of the architecture would be uncomplicated. These findings complement the previous ones by showing that ZTA is technically feasible and user-friendly for the current healthcare organization environment.

The study's main contributions are a novel ZTA reference architecture for cloud, on-premise, and mobile IT developed for healthcare organizations. Furthermore, the new generation of healthcare policy templates provided subtypes to make differentiated access decisions by roles, device states, and risk contexts to protect healthcare data without hindering the healthcare working processes. Performance benchmarking would also give a clear picture of the ROI on the system, compliance readiness, response to threats, and overall operational improvement that the organization was experiencing. That being said, several potential research avenues for the future include the following ideas that could be the next step in expanding the existing research. First, using blockchain for audit trails may provide secure and unalterable records of access and activities, increasing the accountability of data management. Second on the list is the adoption of confidential computing technologies, which could shield the data as they are being used- a security loophole that the current cloud-based systems lack. This would guarantee that patient data are protected in the database not only when it is idle, stored, and when it is moving from one point to another but also when it is being processed. Last, policy engines driven by AI might help form unique or dynamic policy responses to emerging threats, which can be modified in real time depending on the evolving behavior and threat intelligence patterns. All these ideas may enhance the adaptability, sophistication, and resilience of ZTA to become a cornerstone of the next-generation safeguarded healthcare networks.

References

[1] Kindervag, J. (2010). Build security into your network's DNA: The zero trust network architecture. Forrester Research Inc, 27, 1-16.

[2] Rais, R., Morillo, C., Gilman, E., & Barth, D. (2024). Zero Trust Networks: Building Secure Systems in Untrusted Networks. "O'Reilly Media, Inc.".

[3] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information sciences, 305, 357-383.

[4] Firdaus, W., & Sukmaaji, A. (2024). Exploring Opportunities and Challenges in Multi-Cloud and Hybrid Cloud Implementation. Information Technology International Journal, 2(2).

[5] Martiradonna, A. (2023). Zero trust architectures in a multi-cloud environment (Doctoral dissertation, Politecnico di Torino).

[6] Islam, M. R. (2024). Secure Multi-Cloud Architectures: Best Practices for Data Protection. Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023, 6(1), 564-576.

[7] Naik, N., Hameed, B. Z., Sooriyaperakasam, N., Vinayahalingam, S., Patil, V., Smriti, K.,. & Somani, B. K. (2022). Transforming healthcare through a digital revolution: a review of digital healthcare technologies and solutions. Frontiers in digital health, 4, 919985.

[8] Duggal, R., Brindle, I., & Bagenal, J. (2018). Digital healthcare: regulating the revolution. BMJ, 360.

[9] Sriram, R. D., & Subrahmanian, E. (2020). Transforming health care through digital revolutions. Journal of the Indian Institute of Science, 100(4), 753-772.

[10] Franzone, P. C. (2018). The healthcare digital revolution. PKE srl.

[11] Gundu, S. R., Panem, C. A., & Thimmapuram, A. (2020). Hybrid IT and multi-cloud are emerging trends and improved performance in cloud computing. SN Computer Science, 1(5), 256.

[12] Anh, N. H. (2024). Hybrid Cloud Migration Strategies: Balancing Flexibility, Security, and Cost in a Multi-Cloud Environment. Transactions on Machine Learning, Artificial Intelligence, and Advanced Intelligent Systems, 14(10), 14-26.

[13] Greene, A. H., & McGraw, D. (2020). Privacy and Security Challenges of Improved Patient Engagement. In Engage! (pp. 118-128). HIMSS Publishing.

[14] Holmes, J. H. (2016). Privacy, security, and patient engagement: the changing health data governance landscape. eGEMs, 4(2), 1261.

[15] Walters, C. B., & Duthie, E. (2017, November). Patient engagement as a patient safety strategy: Patients' perspectives. In Oncology nursing forum (Vol. 44, No. 6, p. 712).

[16] Mahapatra, B., Krishnamurthi, R., & Nayyar, A. (2019). Healthcare models and algorithms for privacy and security in healthcare records. Security and privacy of electronic healthcare records: Concepts, paradigms and solutions, 183.

[17] Zhang, R., & Liu, L. (2010, July). Security models and requirements for healthcare application clouds. In 2010 IEEE 3rd International Conference on Cloud Computing (pp. 268-275). IEEE.

[18] Raj, P., Raman, A., Raj, P., & Raman, A. (2018). Multi-cloud management: Technologies, tools, and techniques. Software-defined cloud centers: Operational and management technologies and tools, 219-240.

[19] He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing, 2022(1), 6476274.

[20] Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. Sustainability, 14(18), 11213.