International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V73I5P103

Volume 73 Issue 5, 16-29, May 2025


*Original Article*

# Hybrid Approach to Secure Legacy Healthcare Systems: Integrating Zero Trust and Traditional Security Models

Bashayer Alotaibi[1], Samah Alajmani[2]

[1,2]*Department of Cybersecurity, College of Computer and Information Technology, Taif University, Saudi Arabia.*

[1]*Corresponding Author : bashayer.network2022@gmail.com*

Received: 28 November 2024 Revised: 31 March 2025 Accepted: 22 April 2025 Published: 31 May 2025

***Abstract*** *- Increased dependence on technology within healthcare organizations enhances accessibility and advances the operational efficiency of health services through more immediate diagnoses, faster retrieval of patient records, and enhanced communication among healthcare providers. However, with such advancements in technology, the ongoing utilization of outdated systems like Windows XP and Windows 7 within healthcare organizations is a significant cybersecurity risk. These systems are no longer supported, lack security mechanisms, and are increasingly exposed to attacks like ransomware and data breaches. Thus, sensitive data is extremely exposed to security threats, and continuity of healthcare services is compromised. Traditional perimeter security models, which are still widespread in healthcare organizations, are no longer effective in countering modern threats. To address this, the paper proposes a hybrid security approach that integrates Zero Trust Architecture (ZTA) and traditional perimeter security models. The architecture is proposed to safeguard legacy systems that are impossible to replace and ensure patient information remains secure for both remote and internal users. The primary aim of this research is to provide a pragmatic and adaptable solution to reduce cybersecurity risks associated with legacy systems. The suggested architecture was tested virtually to simulate real-world attack scenarios. The findings indicate that the hybrid model is successful in detecting and preventing threats, enhancing visibility, and enhancing security in healthcare environments that rely on legacy infrastructure.*

***Keywords*** *- Healthcare organizations, Legacy systems, Perimeter security model, Security, Zero Trust Architecture (ZTA).*

## 1. Introduction

The use of technology in healthcare is fast increasing, improving access to services for needy communities and patient outcomes. It also improves the quality of care through real-time access to patient information and improved communication among healthcare workers [1]. Some healthcare organizations still employ older operating systems, such as Windows Server 2008, Windows XP, or Windows 7, that do not receive essential security updates anymore. They were created using obsolete coding practices and technologies and without the robust architectural designs and advanced security features of newer systems.

This gap provides a major security vulnerability, which makes legacy systems prime targets of cyberattacks [2], including malware and ransomware. As a result, healthcare-sensitive data is widely exposed to security breaches. The evolving threat landscape has resulted in conventional perimeter security controls not being sufficient enough to stay in pace with increasing regulatory requirements. Increasing rules and more healthcare data breaches have turned trust into a serious risk threat for organizations [3]. The advent of the ZT model has created a tectonic shift in network security. ZTA is not a single principle but a symphony of diverse principles working together to strengthen overall security resilience. This symphony brings together stringent micro-segmentation, continuous authentication, and rigorous access controls into a unified performance that encloses threats and makes it impossible for them to move around across the network [4] laterally. While researches demonstrate that ZT can improve security, many organizations are hesitating due to the cost and complexity of rebuilding their network infrastructure. Within healthcare, resistance is typically caused by the constraints of the use of legacy systems and specialized medical devices [5].

Although ZTA has been the subject of extensive study, its real-world implementation remains challenging due to a lack of practical deployment experience. Furthermore, while some research has explored ZTA in specific areas like multimedia protection, cloud environments and industrial IoT, its effective integration with traditional security models, particularly in the context of legacy systems in the healthcare infrastructure, remains underexplored. This gap highlights the need for practical, tested solutions that integrate ZT principles with existing security frameworks. This study proposes a practical hybrid framework that combines ZTA with traditional

perimeter security models to enhance the protection of irreplaceable legacy systems in healthcare environments. The proposed approach seeks to mitigate cybersecurity threats by strengthening defense mechanisms, improving visibility, and reducing cyber risks associated with outdated infrastructure. This paper is structured in the following manner: A review of the relevant literature is given in Section 2, the suggested model is explained in Section 3, the experimental setup and evaluation are presented in Section 4, and the results and discussion are presented in Section 5. Section 6 concludes the research.

## 2. Literature Review

### *2.1. Healthcare Technology Systems*

Healthcare is a critical aspect of society, and its advancement has consistently been a key focus for policymakers, researchers, and practitioners [6]. Information Technology (IT) has become increasingly essential for managing the massive amounts of data generated by healthcare systems.

IT is now employed across various sectors, including public health institutions, hospitals, clinics, long-term care facilities, and even homes, to reduce medical errors, enhance the quality of care, and improve cost-efficiency through better data management and clinical decision-making. Modern healthcare systems depend on technologies such as EHRs, telemedicine platforms, IoT devices, blockchain, and cloud computing to support both the delivery and protection of sensitive patient information [6].

### *2.2. Legacy Medical Devices Overview*

Legacy systems refer to technologies developed before the adoption of modern software development methodologies. Although outdated, they often continue to hold significant value due to their critical role in supporting healthcare operations and the difficulty or cost associated with their replacement [7]. In IT, a legacy system is typically resistant to updates and integration because it relies on obsolete technologies. Although such systems are no longer being maintained or supported, healthcare organizations, particularly organizations that operate critical environments like intensive care units, continue to use them because of their operating significance.

The prevalence of these systems in healthcare, with 73% of organizations continuing to use legacy systems, creates numerous cybersecurity risks. Modernization is often restricted by cost and compatibility concerns, which limit the possibility of upgrading or replacing these systems.

To mitigate risk, healthcare organizations can quarantine legacy systems from the internet or apply strict access controls. However, these types of controls are usually not adequate, so healthcare environments are still susceptible to cyber attacks despite such controls [8].

#### *2.2.1. Problems Connected to Legacy Systems*

Legacy systems create significant cybersecurity risks because of their outdated technology and lack of advanced security features. The primary risks are [2].

*Outdated Security Protocols*

Legacy systems implement outdated encryption and authentication methods that are not efficient against modern threats that leave them vulnerable to attacks and unauthorized access.

*Inadequate Patch Management*

Most legacy systems are not supported by vendors with updates anymore, so it is challenging to apply timely patches. This leaves known vulnerabilities open and raises the risk of malware infection and security breaches.

*Limited Integration Capabilities*

These systems struggle to integrate with newer systems because of rigid design and nonstandard protocols that render integration expensive and time-consuming.

*Code Vulnerabilities*

Legacy code is usually developed in outdated languages or uses insecure development practices. This makes it more susceptible to exploitation by malware or data loss.

*Insufficient Audit Trails*

Legacy systems lack logging features that render it difficult to monitor user activity, investigate incidents, or meet compliance requirements. This reduces visibility and introduces a greater risk of threats not being detected.

### *2.3. Perimeter-Based Security Model*

According to Northcutt et al. [9], the perimeter is described as the fortified boundary of a network. It includes components such as DMZs, VPN devices, firewalls, IDS, IPS and border routers. As defined by Yuanhang He et al. [10], the perimeter security model is the traditional model based on the concept of "trust but verify," which uses firewalls, IDS, or IPS to divide the network into internal and external segments.

Traditional network topologies, as shown in Figure 1, primarily rely on perimeter-based security, which assumes that threats originate from outside the network. However, once access is gained, internal networks are not typically segmented appropriately, and this allows attackers to move laterally across the network, so this strategy is not sufficient to counter current threats like insider threats and advanced intrusions.

As shown in Figure 2, external threats decreased from 94% in 2011 to 47% in 2021, while internal threats increased from 6% to 53% over the same period. This shift clearly demonstrates that perimeter security models are no longer sufficient to protect against threats originating within internal networks.

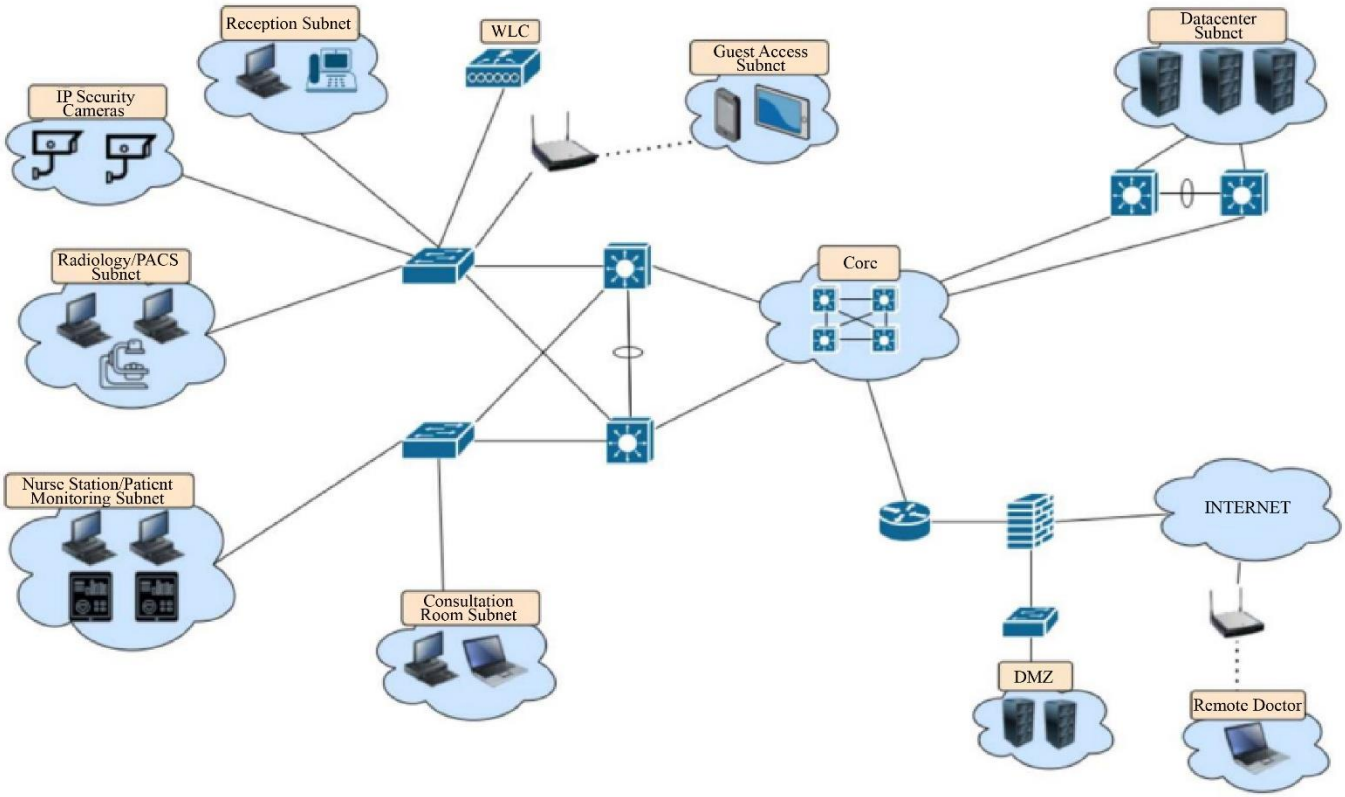


**Fig. 1 Perimeter-based security model [5]**

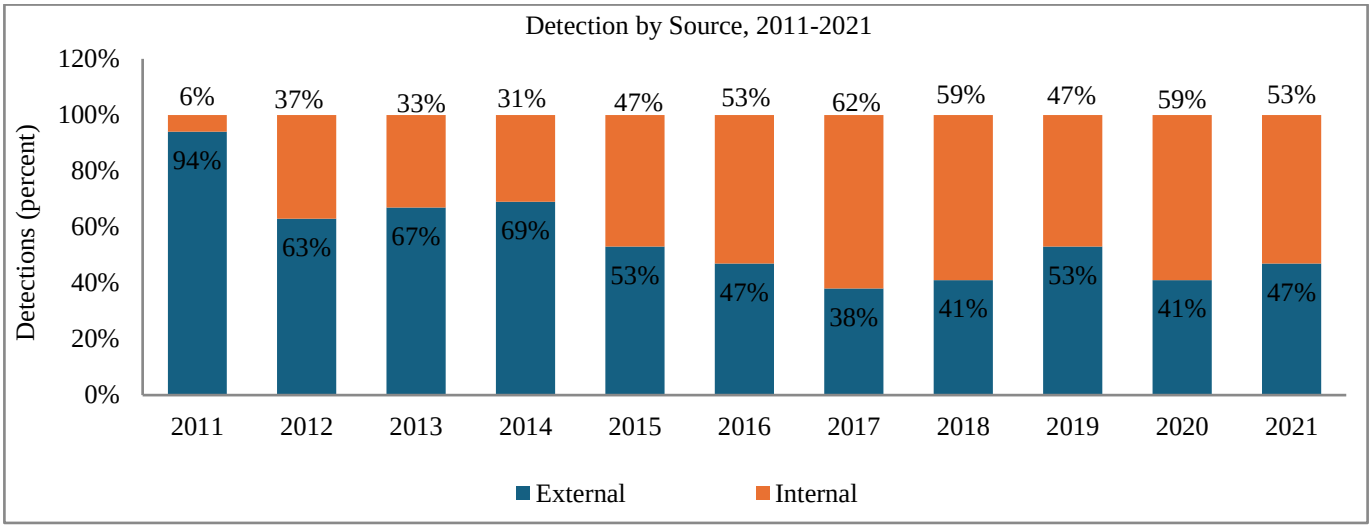


**Fig. 2 Threats detection by source, 2011-2021 [11]**

Although widely used, perimeter security models have several key limitations in addressing modern cybersecurity risks:

*2.3.1. Insider Threats*

These models focus on external threats and often overlook risks from trusted users or compromised accounts. Insiders can bypass controls, leading to data loss, financial damage, and reputational harm.

*2.3.2. Weakness Against Modern Attacks*

Modern cyber threats continue to exploit security weaknesses that make perimeter-based models increasingly ineffective in protecting digital assets [12].

*2.3.3. Lateral Movement*

Lateral movement refers to how attackers move between internal systems after breaching a network [13]. They often avoid detection, access sensitive information, and escalate

control. This is possible because perimeter security models assume that internal traffic is trustworthy. Legacy systems and outdated security models continue to expose healthcare organizations to significant cyber risks. A 2021 Kaspersky report revealed that only 22% of healthcare organizations worldwide use up-to-date software on all medical equipment, while 73% rely on legacy operating systems, increasing vulnerability to threats. Additionally, 50% of healthcare institutions have experienced data leaks, DDoS, or ransomware attacks [14]. Another survey found that 78% reported at least one cybersecurity incident in the past year, with over 60% facing moderate to severe impacts on care delivery and patient safety, over a quarter paid ransoms, and more than a third incurred financial losses exceeding $1 million [15].The 2017 WannaCry ransomware attack affected 34% of NHS trusts in England, disrupting services across 81 trusts and over 600 primary care organizations due to unpatched systems, resulting in widespread service disruptions [16]. Increasing constraints of perimeter-based security that include weak internal controls and greater exposure to advanced threats highlight the need for a more adaptive security strategy. This shift has brought attention to ZTA as a model capable of addressing these ongoing challenges.

### *2.4. Zero Trust Model*

The concept of ZT was created by the Jericho Forum in 2007 [17], which proposed the concept of de-perimeterization, to help overcome the restrictions of traditional security perimeters. Their report suggested that security needed to be pervasive, scalable and flexible in untrusted environments. Subsequently, in 2010, John Kindervag proposed the term "Zero Trust", highlighting that no network traffic is to be trusted by default, irrespective of where it comes from [18]. This method is centered on protecting data from the inside, leading to a more efficient and streamlined security model. ZTA departs from perimeter models that rely on internal trust rather than treating all networks—internal or external—as untrusted. It is a strategic method directed towards safeguarding an organization's assets by constantly checking and authenticating every access request as if it came from an untrusted source. According to research from the NIST and related literature [19, 20] ZTA employs a number of fundamental principles to accomplish its mission.

#### *2.4.1. Location*

All-access requests, both internal and external to the network, are required to go through the same rigorous security evaluation. Physical location does not mean trust; devices and users are governed by the same policies, providing consistent access control regardless of where the connection is coming from.

#### *2.4.2. Micro-Segmentation*

Resources are segmented into smaller blocks managed by gateway appliances like switches or NGFWs. User, asset, or service access is dynamically controlled via these gateways. Alternatively (or in Addition), host-based segmentation can be enforced using endpoint firewalls or agents to place access policy at the device level.

#### *2.4.3. Just-in-Time Access (JITA)*

Each request to access must be authenticated, approved and assessed in real time depending on policies in place at the time of making the request. This reduces the risk of long-term access and privilege misuse.

#### *2.4.4. Just Enough Access (JEA)*

Users, applications or systems receive only the minimum of permission required to complete certain operations. This is according to the principle of least privilege, where access is restricted to only what is needed to support the role or function.

#### *2.4.5. Continuous Diagnostics and Mitigation (CDM)*

Regular scanning of assets to decide their posture with respect to security, updating them and responding to threats in real-time. It includes identifying abnormal behavior, response automation such as isolation or policy modification and changing control made according to system feedback in real-time.

#### *2.4.6. Encryption of Communication*

Confidential information is shielded with encryption into non-readable forms. With this, if data is intercepted, it becomes impossible to decipher or utilize them without licensed decryption that keeps communications secure within every network environment. As demonstrated by Figure 3, ZTA is made up of logical components that apply policies for access and control communications between users, devices and resources.

These components are organized into two planes: the control plane, which manages authentication and authorization decisions and the data plane, which transmits application data according to the established security rules [19].

At the heart of the control plane is the PDP, which consists of two components: the PE and the PA. The PE evaluates access requests using organizational policies, user identity, device posture and threat intelligence. Based on this evaluation, it determines whether to grant, deny or escalate access. The PA enforces the PE’s decisions by establishing or terminating communication paths and issuing credentials to clients [19]. The PEP serves as the final checkpoint and enforces the access control decisions made by the PE and PA. It monitors and regulates connections between subjects and resources and is considered the core of the data plane [21]. The PEP may include a client-side agent and a gateway, which together ensure that access is granted only under the correct security conditions [21].

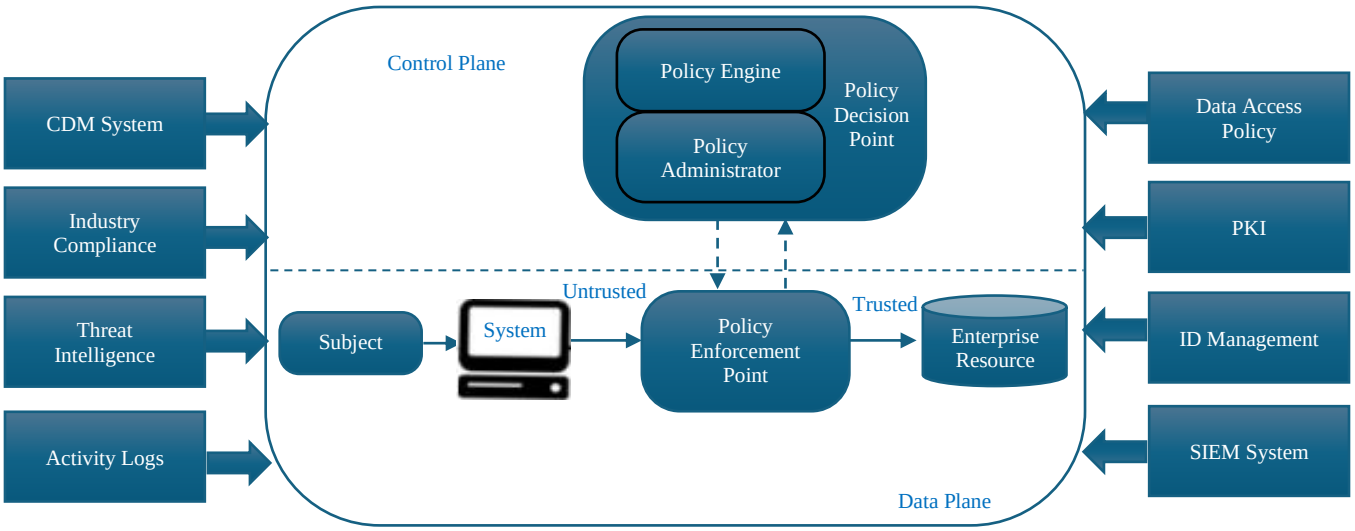


**Fig. 3 Core zero trust logical components [19]**

When a request is made, the PEP intercepts it and passes it to the PA, who forwards it to the PE for evaluation. Once a decision is made, the PA communicates the outcome to the PEP, who then either grants access, requests further authentication, or denies the session based on the current security context.

ZTA relies on a variety of internal and external data sources to support real-time access decisions. These sources provide the Policy Engine with contextual insights to assess risk and enforce security policies effectively [19].

- CDM system which monitors asset configurations, software integrity, patch status, and the presence of vulnerabilities.
- Industry compliance system helps organizations align with sector-specific regulations, such as those in healthcare and finance.
- Threat intelligence feeds provide data on newly discovered threats, including malware, vulnerabilities, and reported incidents, allowing the Policy Engine to block access to compromised resources.
- System activity logs offer visibility into network traffic, user behavior, and resource usage.
- Data access policies define user privileges and roles.
- Public Key Infrastructure (PKI) supports secure authentication through certificate management.
- Identity management system maintains and governs user credentials and permissions.
- SIEM systems collect and analyze security events, helping to detect and prevent potential threats.

ZTA is not a complete replacement for existing systems but a progressive shift from traditional models [19]. Organizations can gradually integrate ZT principles, update their processes, and deploy supporting technologies to secure critical assets better.

### *2.5. Related Works*

Several studies have investigated the adoption of ZTA as a security framework, analyzing its implementation strategies and effectiveness in addressing modern cybersecurity challenges. This section presents existing approaches and related studies. Tyler and Viana [5] proposed a ZT framework tailored for healthcare organizations to address security challenges associated with legacy systems and medical appliances. The model proposes microsegmentation through firewall clustering, where physical firewalls are deployed in front of individual medical devices to isolate traffic and enforce access controls.

This approach was validated through simulations using Cisco Modelling Labs (CML), which demonstrated that a compromised host within the LAN could be effectively contained to prevent lateral movement. As a result, firewalls were selected as the primary security control, and clustering was used to provide redundancy while maintaining acceptable performance. However, testing showed that the failure of one firewall in the cluster led to a 55% packet loss after convergence, raising concerns about reliability in critical healthcare environments.

In addition, while this segmentation improved network isolation, the lack of centralized access control, network-based authentication (e.g., 802.1X or MAB), and policy orchestration tools such as Cisco ISE limits scalability and flexibility. The inability of visibility mechanisms such as compliance posture checks, centralized event correlation and system health monitoring also limits the framework's ability to support an extensive Zero Trust deployment in alignment with the security and operational needs of healthcare environments.

Paul and Rao [22] introduced a ZT framework tailored for smart manufacturing environments, which aims to protect

communication channels between manufacturing devices and control systems. The model employs micro-segmentation through firewall-based network isolation, effectively separating Operational Technology (OT) from Information Technology (IT) domains. Inter-phase communication is segmented through rule-based filtering implemented on a centralized firewall where rules are configured using a least-privilege approach to control inter-device communication within the manufacturing environments.

Additionally, RBAC policies are applied via IAM tools to ensure that user-level isolation and access credentials for IT and OT domains are managed. Compliance enforcement is achieved using Endpoint Compliance Management systems, which validate device posture against predefined policies, including antivirus status, OS version and patch level. Cloud connector is also included in the model to facilitate safe communication with cloud storage, and all remote access to the OT network is managed through a PRA jump server with VPN. While providing a well-defined model for industrial environments, the proposed framework lacks several important capabilities to defend legacy healthcare systems.

It lacks SIEM or performance monitoring, features that are necessary to maintain visibility into legacy systems. Additionally, the absence of network-level authentication (i.e., 802.1X or MAB) and its lack of testing or performance validation further limit its deployment in healthcare environments where operational continuity is critical to patient safety. Accordingly, while the model does address foundational ZT fundamentals, architectural limitations reduce its effectiveness for healthcare networks on legacy infrastructure.

Zanasi et al. [23] defined a ZTA for Industrial Control Systems (ICS) aimed explicitly at supporting cybersecurity needs in the context of IT/OT convergence and vulnerability to legacy infrastructure. The methodology takes advantage of access proxies to enable dynamic context-aware access controls and NGFWs for segmenting and preventing lateral movement. The design involves a trust algorithm that continually analyzes user and device identity, risk posture, and environmental context.

A framework deployment validated the model to be effective in preventing unauthorized access and containing threats in ICS networks. However, while it is stronger at protecting industrial settings, the framework lacks some vital components required in healthcare legacy settings, such as EDR, real-time performance monitoring and centralized event correlation via SIEM. Moreover, the absence of scalability and availability of design elements reduces the model's suitability for deployment in healthcare environments.

Rahman et al. [24] proposed a ZTA for MSMEs involving MFA, microsegmentation and IDPS to mitigate cybersecurity threats. Their architecture effectively demonstrated a 49.5% decrease in security incidents post-implementation, leading to an enhanced cybersecurity state. Microsegmentation was used to isolate the smart front office and backend system while controlling traffic via IDPS.

However, the research also points out some implementation challenges that vary from limited budget to ongoing training. Furthermore, the absence of EDR, performance monitoring, centralized event correlation using SIEM and network-layer authentication techniques like 802.1X or MAB limits the framework to achieve the visibility, compliance and resiliency requirements needed to protect legacy systems on important healthcare infrastructure.

Habash and Ibrahem [25] proposed a ZTA of enterprise networks aimed at offering increased security by reducing insider threats and keeping attackers out. The architecture uses identity and access control approaches on the basis of AD, group policy enforcement at the domain level and privilege limitations to limit unauthorized action and privilege escalation in the network. Experimental validation was conducted in EVE-NG and confirmed that internal users could not implement unauthorized modifications without administrator consent, successfully evading insider attacks.

Although it is robust in preventing unauthorized adjustments and confirming administrative access, the architecture lacks the fundamental components required for securing legacy health systems in healthcare. Significantly, it does not have the MFA, EDR or performance monitoring tools necessary for visibility and threat mitigation on outdated infrastructures.

Secondly, the absence of SIEM and network access control features such as 802.1X or MAB limits the framework's ability to establish centralized, adaptive access control and compliance monitoring. These limitations indicate that the model is not properly equipped to handle the general security requirements of legacy-dependent health networks. The referenced studies demonstrate the implementation of ZTA in various sectors with emphasis on principles like continuous authentication, identity-centric security and micro-segmentation.

## 3. The Proposed Model

The following section introduces the proposed security model, as depicted in Figure 4, intended to secure healthcare organizations based on legacy systems. The model integrates both ZTA principles and conventional perimeter security controls aimed at combating contemporary cybersecurity issues.

The following subsections outline unique aspects of the model that work together to create a strong and efficient security model.

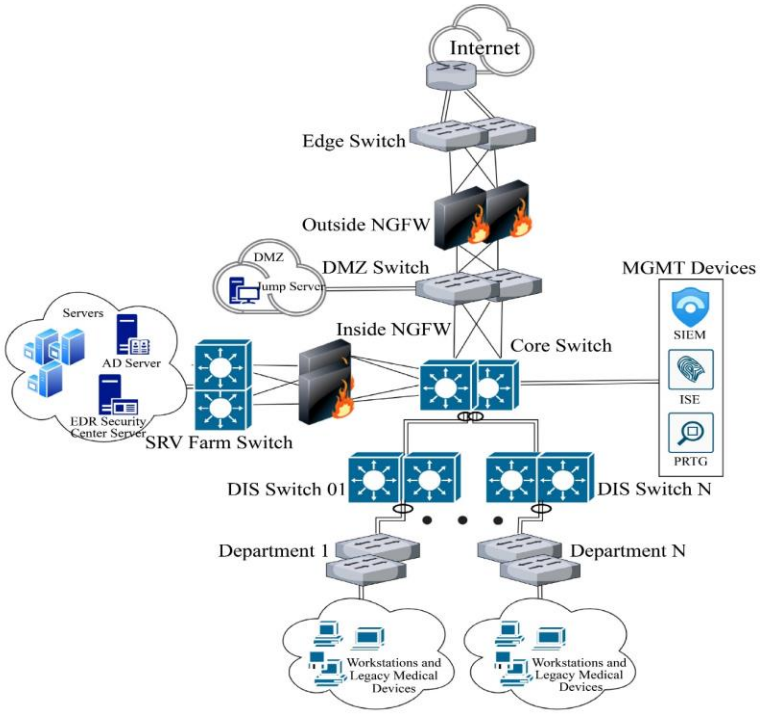


**Fig. 4 The proposed model**

### *3.1. Network Segmentation and Access Control*

This section focuses on network segmentation and access control as a key aspect of the proposed model that builds isolated zones to improve security and enhance threat detection, as depicted in Figure 5.

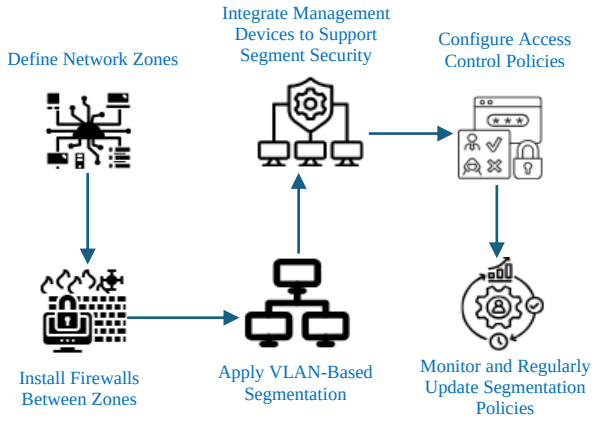


**Fig. 5 Network segmentation and access control**

It begins with the design of network zones, such as Campus Zone, Server Farm Zone, and DMZ, to perform a particular function to isolate each part of the network according to security needs. Firewalls are inserted between zones, such as the external NGFW between the internal network and the internet and the internal NGFW between the Server Farm Zone and the Campus Zone, to limit traffic and threat mitigation. VLAN is employed to create segregated virtual segments for every department, creating secure and organized communication. Crucial key management appliances, like ISE, PRTG and SIEM, are employed to apply access policies and provide centralized visibility within segments. Access control policies are configured through ACLs to limit inter-segment traffic to authorized communications. Finally, segmentation policies are under continuous monitoring and re-tuned to continue being compliant with evolving security threats, maintaining tight boundaries between network zones.

### *3.2. Identity and Access Management*

This section addresses IAM as an essential aspect of the proposed model that enhances network security through identity-based access controls and MFA, as depicted in Figure 6. IAM leverages Cisco ISE, AD and MFA for the purpose of enforcing rigorous access policies to permit only authenticated and authorized users to access critical resources on the network. To accomplish this, 802.1X authentication is configured on network switches that ruire devices and users to authenticate before granting network access. Cisco ISE, when integrated with AD, centralizes identity management by verifying user credentials and enforcing access policies. MFA adds a layer of security through a TOTP combined with AD credentials that offer robust verification for network access. Cisco ISE applies predefined access control policies based on user identity, roles, and device types, restricting access to needed resources while protecting sensitive assets. Identity and access policy management centralized by Cisco ISE allows for easy control and update from a single location to provide consistent and secure access management across the network.

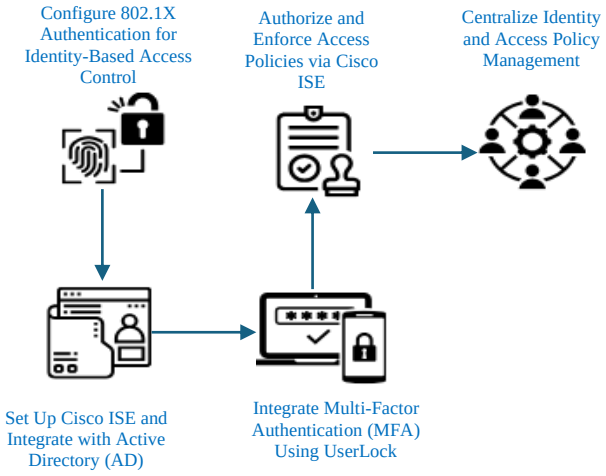


**Fig. 6 Identity and access management**

### *3.3. Continuous Monitoring and Analytics*

This section describes continuous monitoring and analytics as a core aspect of the suggested model. This aspect involves real-time monitoring and analysis of network traffic for greater threat detection and network stability. As depicted in Figure 7, this approach has total visibility to all areas in the network, using specialized systems for analyzing traffic and security incidents that all contribute to a secure organizational environment.

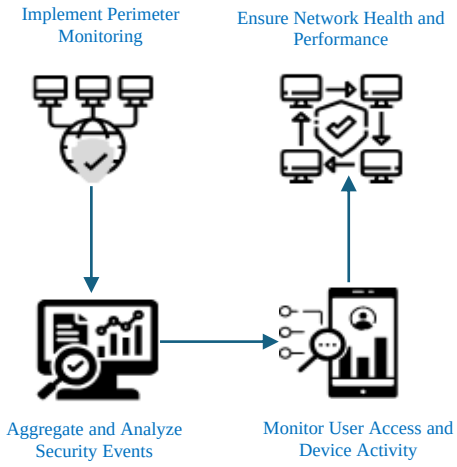


**Fig. 7 Continuous monitoring and analytics**

Perimeter security is maintained by filtering traffic in the points of entry using firewalls to record events and trigger alerts on unauthorized access attempts or malicious activity. Security events are aggregated and analyzed by a centralized SIEM system that collects logs from many network sources, detects anomalies and facilitates early detection of potential incidents. Also, user activity and device activity are tracked with the assistance of Cisco ISE, which implements identity-based policies and identifies any unauthorized access. Network health and performance are maintained under observation using the PRTG system, which gives information about the devices' status and troubleshoots potential vulnerabilities for network reliability assurance.

### *3.4. Breach Detection and Response*

In this section, breach detection and response are discussed as critical aspects of the proposed model, where focus is given to the detection, containment, and mitigation of future security incidents across the network. As shown in Figure 8, this process makes use of a number of security controls as well as real-time alerting mechanisms to reinforce network defenses.


**Fig. 8 Breach detection and response**

Perimeter defenses are configured to detect and block suspicious activity based on preconfigured security policies and initiate alerts for any potential compromise. Centralized collection and analysis of security logs across different sources correlate information to detect patterns and initiate real-time alerts that enable rapid incident response. Also, continuous monitoring of user and device behavior is performed to detect anomalies, isolate compromised devices, and prevent lateral movement, which ensures threats are contained within specific segments.

### *3.5. Secure Remote Access*

This section explores Secure Remote Access as a critical aspect of the proposed model, emphasizing the protection of remote connections to ensure data security and controlled network access. As shown in Figure 9, secure remote access is facilitated by implementing a VPN to establish encrypted communication channels, protect sensitive information during transit, and maintain confidentiality. A dedicated jump server is deployed to regulate and manage remote user connections that guarantee the network can only be accessed by authorized and authenticated users. Continuous monitoring and logging of remote access sessions provide real-time visibility to enable the detection of unusual behavior and reinforce the security of remote interactions.

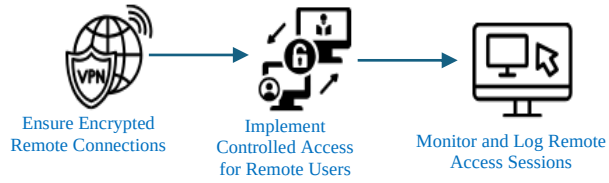


**Fig. 9 Secure remote access**

### *3.6. Endpoint Detection and Response (EDR)*

This section emphasizes EDR as a key aspect of the proposed model that improves endpoint security. As illustrated in Figure 10, EDR focuses on continuous monitoring and real-time threat response directly on individual devices. EDR software is deployed across all end-point machines for automatic response against suspicious activities and ensures local detection capability. Single-console centralized management of EDR policies enforces uniform security across the network that allows rapid response when threats are detected. The system also logs detailed endpoint activity and security event data, with essential data accessible for forensic examination and incident response.

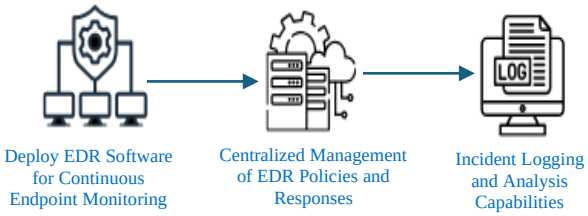


**Fig. 10 Endpoint detection and response (EDR)**

The proposed model is designed to offer strong protection and performance by meeting critical operational needs, including scalability to enable network growth, robustness against cyber threats and evolving threat landscapes and availability to guarantee continuous access to critical resources. These requirements all establish critical standards for making the framework scalable, robust, and available, meeting the specific needs of healthcare organizations.

## 4. Experimental Results

### *4.1. Experimental Setup*

The experiment setup was designed to simulate a healthcare network environment with legacy systems in order to measure the effectiveness of the proposed security framework presented in the earlier section. The topology included three separate zones: campus zone, server farm zone, and DMZ, as described in the proposed model. Every zone was critical in the delivery of a safe and segmented network environment where the unique requirement of healthcare organizations was addressed. EVE-NG was employed as the emulation platform for the network to build and set up the virtualized network topology, incorporating key network devices like Cisco routers, switches, FW, servers, and key management devices like Cisco ISE, SIEM systems, and PRTG.

The campus zone follows a three-layer design: access, distribution and core. VLAN-based segmentation was used to allocate separate VLANs per department, separating traffic and imposing custom security policies. The Access Layer used 802.1X authentication for identity-based access control in combination with other methods to authenticate and secure device connections, allowing only authorized and compliant devices to connect to the network. At the Distribution Layer, inter-VLAN ACLs were used to limit inter-departmental communication, enforcing strict traffic flow according to security policies. The Core Layer provided connectivity between distribution switches and critical management devices, such as Cisco ISE, SIEM, and PRTG, unified network monitoring, identity-based access control, and policy enforcement throughout the network.

The server farm zone was designed to preserve the key assets, such as the AD server and Kaspersky endpoint management server. The Kaspersky server monitored the EDR abilities, ensured real-time visibility, automated detection of threats, and quick reaction to security alerts directly at the device level. These assets were placed in a dedicated VLAN, with NGFW policies that closely govern access from other segments to protect sensitive operations and critical infrastructure. Other security controls involve strict firewall policies and dedicated access controls that provide protection against unauthorized access while ensuring that the required functionality is available for healthcare services.

The DMZ provided secure external access and had a jump server as a secure entry to internal resources. To further secure remote interactions, VPN tunnels were used to encrypt in-transit data, which maintains confidentiality and integrity during communication. The firewall policies restricted access to necessary protocols such as RDP and SSH and allowed only authenticated and authorized access. In addition to that, strong logging and monitoring controls were implemented in order to examine and track attempts made to access and offer visibility and security during external connections.

This setup also included advanced configurations for IAM, integrating Cisco ISE with AD and MFA. These measures ensured that only authenticated users with verified credentials could access critical resources that align with ZT principles. Monitoring and analysis were ongoing through SIEM and PRTG to make real-time evaluations of network traffic, identify any anomalies, and trigger alerts about possible security violations. For detection and response to incidents, firewalls, Cisco ISE and SIEM were set to automatically identify and quarantine malicious traffic, enforcing tight security policies to quarantine threats and lateral movement.

The experimental setup, structured according to the model developed, provided a basis for testing and verifying the proposed security framework under real-time conditions.

### *4.2. Experimental Evaluation*

To assess the performance of the proposed security framework, the subsequent sections give experimental analyses carried out to validate the model to detect and respond to attacks against legacy systems.

*4.2.1. DoS Attack Simulation*

For the evaluation of the effectiveness of the proposed security model against DOS threats, a TCP SYN flood attack was simulated using the Hping3 tool on Kali Linux. This attack exploits the TCP three-way handshake process by sending a large volume of SYN packets without completing the handshake, which consumes system resources and renders the system unresponsive to legitimate connection attempts. The attack targeted a Windows 7 machine, simulating a legacy system vulnerable to resource exhaustion due to outdated security mechanisms. To evaluate the proposed model under escalated DOS conditions, three SYN flood scenarios were simulated, each varying in packet size and transmission interval. These scenarios were designed to reflect different levels of attack intensity that target a legacy Windows 7 system. As shown in Figure 11, the configuration highlights the variation from low to high transmission rates to assess the model's effectiveness in addressing diverse SYN flood patterns. The SYN flood attack was detected and prevented across the layers of the security mechanisms. The firewall identified the high volume of SYN packets coming from the attacker's IP as a critical threat and responded accordingly, as shown in Figure 12.

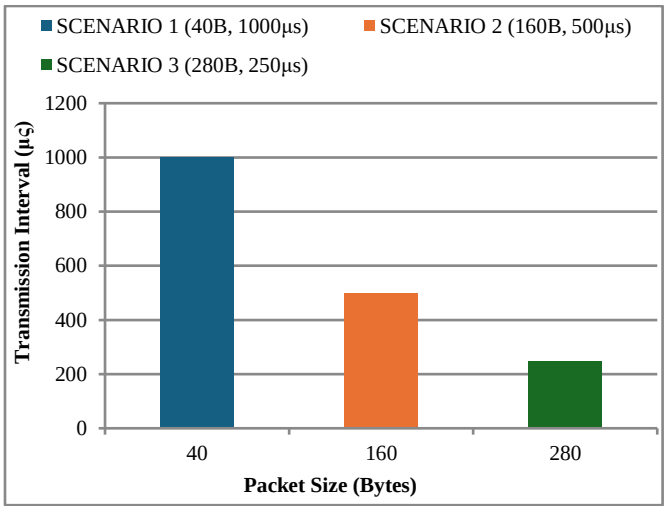


**Fig. 11 Comparison of packet sizes and transmission intervals in syn flood attack scenarios**

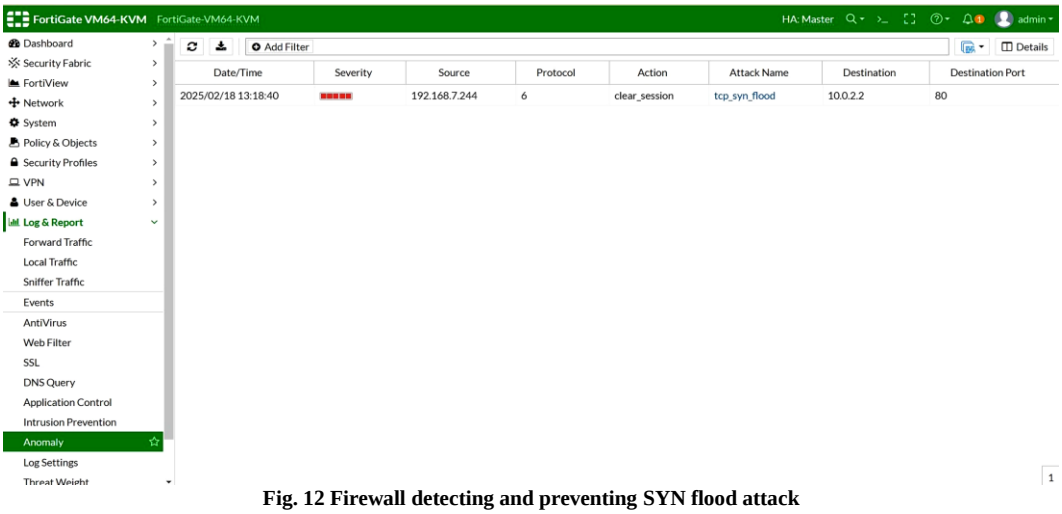


**Fig. 12 Firewall detecting and preventing SYN flood attack**

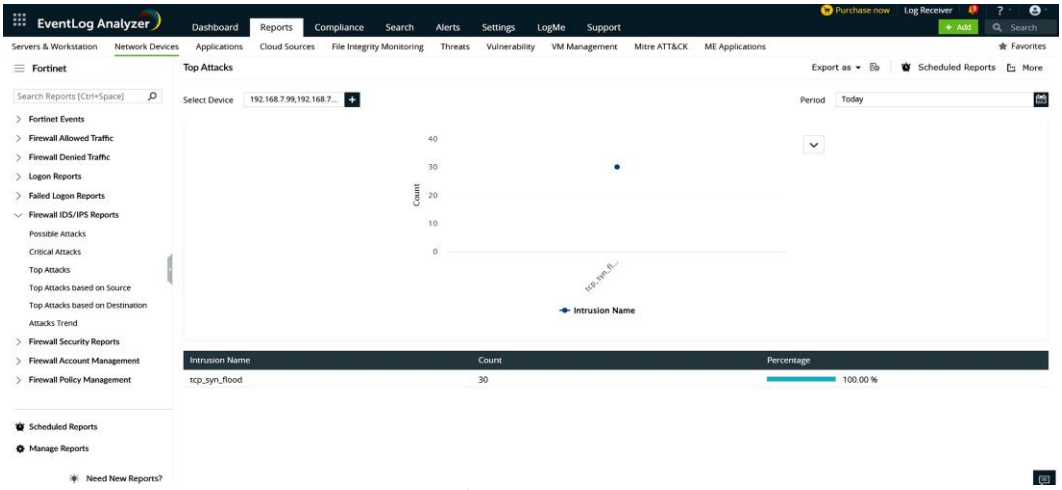


**Fig. 13 SYN flood session alerts in SIEM**

At the same time, the SIEM system recorded multiple alerts related to SYN flood activity, as shown in Figure 13. These alerts were associated with abnormal traffic patterns and highlighted several critical anomalies resulting from excessive SYN requests. Additionally, PRTG Network Monitor provided real-time performance metrics during the attack, which confirmed that the targeted system maintained stable operation without signs of resource exhaustion, as shown in Figure 14. The experimental results confirm the effectiveness of the proposed security model in detecting and preventing SYN flood attacks. The attack was prevented through coordinated security mechanisms involving rate-limiting at the firewall, traffic behavior analysis by the SIEM, and real-time performance monitoring through PRTG, all of which contributed to securing legacy systems. At the host level, EDR mechanisms enforced security policies against abnormal connection attempts, while Control Plane Policing (CoPP) preserved the stability of network infrastructure by protecting control plane functions from excessive traffic. The inclusion of ZTA principles continued to offer security for legacy systems through constant verification of traffic activity and restriction of suspect connection attempts, ensuring that attempts at DOS were intercepted and contained without affecting the functional integrity of the core system.

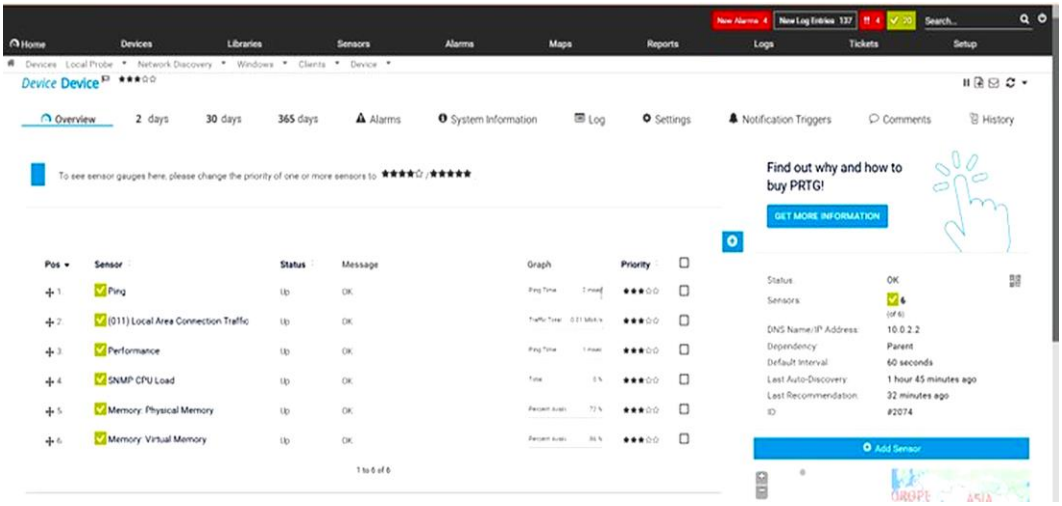


**Fig. 14 Monitoring metrics for endpoint**

To ensure the consistency and accuracy of these observations, each attack scenario was executed three times. During the testing, initiation time, detection and response time, and response delay were monitored. In each of the experiments, the suggested model was able to record an instantaneous response time of 0 seconds, which validates its ability to recognize and respond to DOS attacks in legacy healthcare systems instantly.

*4.2.2. DNS Spoofing Attack Simulation*

DNS Spoofing, alternatively known as DNS Poisoning, is an attack in which an adversary manipulates DNS responses to redirect legitimate traffic to improper destinations. The attack exploits vulnerabilities within the DNS resolution procedure that allows intruders to intercept or manipulate queries. Legacy systems such as Windows 7 are particularly vulnerable to DNS spoofing since they rely on LLMNR and NBT-NS. These protocols lack robust authentication mechanisms that leave them exposed to poisoning attacks.

Responder was used in this test to conduct a DNS spoofing attack against an internal Windows 7 host. The attacking machine was set to listen for localhost DNS queries and respond with spoofed records to send clients to improper destinations by poisoning the name resolution process. LLMNR and NBT-NS were disabled through Group Policy (GPO) in the proposed security framework as part of the security mechanism to avoid unauthorized name resolution responses. The GPO settings applied guaranteed that the system was no longer dependent on these protocols, thus preventing exploitation via spoofed responses.

Limiting unauthorized DNS communication is critical to reducing attack vulnerability and blocking attackers from injecting malicious responses, by suggested framework imposes DNS filtering policies that guarantee endpoints only validate and accept approved responses. These types of restrictions reduce the exploitation rate of attacks through counterfeit replies. Unauthorized attempts to connect were effectively blocked, and the SIEM system, as illustrated in Figure 15, logged several denied communications with the attacker's DNS server.

These results support the effectiveness of the proposed security model in preventing DNS spoofing attacks; by blocking illegal DNS communications and detecting malicious behavior through SIEM logging, the framework prevented the threat of name resolution poisoning. The use of DNS filtering rules and real-time network monitoring ensured that responses with spoofed IP addresses were denied.

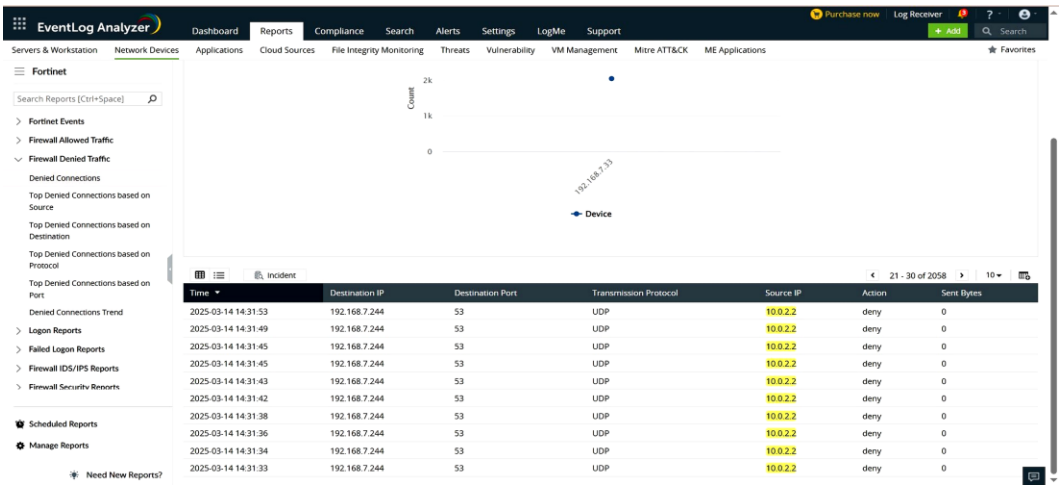


**Fig. 15 SIEM log of blocked DNS redirection attempts**

Implementation of ZTA concepts furthered prevention by applying stringent access control to DNS communication. Processing of DNS was limited to trusted and approved systems, disallowing unauthorized parties from transmitting or receiving queries. This layered security preserved the integrity of DNS transactions and effectively reduced the threat of successful manipulation or redirection. To verify these findings, the attack was run in three experiments, with each demonstrating a 0-second response delay that shows the model's ability to detect and respond to spoofed DNS responses in real time.

## 5. Results and Discussion

The findings verify that the framework enhances overall security and protects legacy systems from a wide range of threats. Segmentation, access control policies and mechanisms of ongoing monitoring at the network level together prevented unauthorized access, controlled traffic flow and gave real-time visibility to possible threats. At the host level, EDR provided real-time monitoring and automated response against suspicious activity, successfully targeting advanced threats to legacy systems. The architecture was also designed with a focus on availability, embedding redundancy features into it that make the network highly available and provide uninterrupted access to important healthcare systems and services. Second, scalability was built into the design as a fundamental aspect that supports effortless scaling to support more users, devices and departments without security compromise. By integrating these concepts, the framework safeguards significant systems, protects confidential information and maintains uninterrupted healthcare services.

ZTA is not a product but rather a strategic design that brings together various security aspects like access control mechanisms, real-time analytics capabilities, identity-proofing solutions and complete endpoint protection. The architecture supports customization as per organizational needs and policies, including defining rules for access and security control customization depending on operational procedures and compliance needs based on healthcare environments. The adaptability of the model allows it to fit each healthcare organization's unique operational needs and device integrations.

However, implementing this model is not simple. It poses risks like the expense of purchasing and maintaining advanced technologies, the need for skilled personnel to manage complex systems, and the time required for successful deployment. Management of the different components within the framework necessitates staff having specialized knowledge for optimal alignment and performance. These training requirements, time, and effort add to the overall deployment effort.

But, through proper planning and resource management, these challenges can be overcome, eventually making the security posture of healthcare organizations better; as much as the simulation results verify the framework efficacy as a proof of concept, further real-world experimentation is required to refine the model, address practical implementation concerns and accommodate the operational demands of healthcare environments.

## 6. Conclusion

Healthcare infrastructures have changed significantly, supporting quicker diagnoses and immediate patient record access, improving the level of care and the efficiency of the care process. However, the majority of healthcare organizations are still utilizing legacy systems that lack modern security features, exposing sensitive patient information to attacks and operational disruptions. Legacy perimeter security models are now outdated in addressing current threats, including insider threats and lateral network traversal, necessitating more robust and dynamic security systems. In this paper, a hybrid security model that blends ZTA with the conventional perimeter models is introduced to enhance access control, threat detection in real-time, and data protection for internal and remote access. The framework was

experimentally tested in a virtual setup, and the simulated attacks were detected and prevented, as it was found effective in protecting legacy systems. While further real-world testing will be needed to address practical deployment challenges, the results confirm that the proposed model provides a good foundation for strengthening the cybersecurity posture of healthcare organizations and protecting and preserving the integrity of critical healthcare services.

## References


[1] Shipu Debnath, "Integrating Information Technology in Healthcare: Recent Developments, Challenges, and Future Prospects for Urban and Regional Health," *World Journal of Advanced Research and Reviews*, vol. 19, no. 1, pp. 455-463, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Vijayasekhar Duvvur, "Securing the Future: Strategies for Modernizing Legacy Systems and Enhancing Cybersecurity," *Journal of Artificial Intelligence & Cloud Computing*, vol. 1, no. 3, pp. 1-3, 2022. [CrossRef] [Publisher Link]

[3] George A. Gellert et al., "Zero Trust and The Future of Cybersecurity in Healthcare Delivery Organizations," *Journal of Hospital Administration*, vol. 12, no. 1, pp. 1-8, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Muhammad Jamshid Khan, "Zero Trust Architecture: Redefining Network Security Paradigms in the Digital Age," *World Journal of Advanced Research and Reviews*, vol. 19, no. 3, pp. 105-116, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Dan Tyler, and Thiago Viana, "Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture," *Applied Sciences*, vol. 11, no. 16, pp. 1-18, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Parisasadat Shojaei, Elena Vlahu-Gjorgievska, and Yang-Wai Chow, "Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review," *Computers*, vol. 13, no. 2, pp. 1-25, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] "International Conference on Communication Technologies (ComTech 2017)," *Institute of Electrical and Electronics Engineers (IEEE)*, Rawalpindi, Pakistan, pp. 1-219, 2017. [Publisher Link]

[8] Brian Eastwood, Tips for Health Systems on Managing Legacy Systems to Strengthen Security, HealthTech Magazine, 2024. [Online]. Available: https://healthtechmagazine.net/article/2023/01/tips-health-systems-managing-legacy-systems-strengthen-security

[9] Stephen Northcutt, *Inside Network Perimeter Security*, 2nd ed., Sams, 2005. [Google Scholar] [Publisher Link]

[10] Yuanhang He et al., "A Survey on Zero Trust Architecture: Challenges and Future Trends," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] M-Trends 2022 Mandiant Special Report, Executive-Summary, 2022. [Online]. Available: https://mandiant.widen.net/s/kxbbdppzzk/m-trends-2022-executive-summary

[12] Saeid Ghasemshirazi, Ghazaleh Shirvani, and Mohammad Ali Alipour, "Zero Trust: Applications, Challenges, and Opportunities," *arXiv*, pp. 1-23, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Grant Ho et al., "Hopper: Modeling and Detecting Lateral Movement (Extended Report)," *arXiv*, pp. 1-20, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Kaspersky Finds 73% of Healthcare Providers Use Medical Equipment with a Legacy OS, Kaspersky, 2024. [Online]. Available: https://usa.kaspersky.com/about/press-releases/kaspersky-finds-73-of-healthcare-providers-use-medical-equipment-with-a-legacy-os

[15] Rising Cyber Incidents Challenge Healthcare Organizations, Help Net Security, 2023. [Online]. Available: https://www.helpnetsecurity.com/2023/08/30/cyber-incidents-challenge-healthcare-organizations/

[16] Department of Health, Investigation: WannaCry cyber-attack on the NHS, UK National Audit Office, pp. 1-35, 2018, [Online]. Available: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

[17] Jericho Forum™ Commandments, The Need for Trust, 2007. [Online]. Available: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

[18] John Kindervag, Build Security Into Your Network's DNA: The Zero Trust Network Architecture, paloaltonetworks, pp. 1-27, 2010. [Online]. Available: https://media.paloaltonetworks.com/documents/Forrester-Build-Security-Into-Your-Network.pdf

[19] Scott Rose et al., "Zero Trust Architecture," *National Institute of Standards and Technology*, pp. 1-59, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Malcolm Shore, Sherali Zeadally, and Astha Keshariya, "Zero Trust: The What, How, Why, and When," *Computer Society*, vol. 54, no. 11, pp. 26-35, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Hongzhaoning Kang et al., "Theory and Application of Zero Trust Security: A Brief Survey," *Entropy*, vol. 25, no. 12, pp. 1-26, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Biplob Paul, and Muzaffar Rao, "Zero-Trust Model for Smart Manufacturing Industry," *Applied Sciences*, vol. 13, no. 1, pp. 1-20, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Claudio Zanasi et al., "A Zero Trust Approach for the Cybersecurity of Industrial Control Systems," *2022 IEEE 21st International Symposium on Network Computing and Applications (NCA)*, Boston, MA, USA, pp. 1-7, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Abdul Rahman et al., "Implementation of Zero Trust Security in MSME Enterprise Architecture: Challenges and Solutions," *Sinkron: Journal and Research of Informatics Engineering*, vol. 8, no. 3, pp. 2077-2087, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Rania M. Habash, and Mahmood K. Ibrahem, "Zero Trust Security Model for Enterprise Networks," *Iraqi Journal of Information and Communication Technology*, vol. 6, no. 2, pp. 68-77, 2024. [CrossRef] [Google Scholar] [Publisher Link]