iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

A ZERO TRUST DRIVEN IDENTITY AND PRIVILEGED ACCESS MANAGEMENT FRAMEWORK FOR NIH REGULATED HEALTHCARE ENVIRONMENTS

Prudhvi Ananthula
CISM, CISA, Master of Science in Computer Science, University of Michigan
North Brunswick, New Jersey, USA

ORCID: 0009-0003-5458-8989
https://orcid.org/0009-0003-5458-8989
prudhvia16@gmail.com

DOI: https://doi.org/10.5281/zenodo.20062624

ABSTRACT
Healthcare facilities under the jurisdiction of the National Institutes of Health (NIH) represent some of the most sensitive biomedical and patient information sources, and thus they are some of the biggest targets of more and more advanced cyber threats. Conventional perimeter-based security paradigms cannot adequately cope with threats posed by insider threats, credential abuse, and distributed access in hybrid infrastructures. This paper suggests a framework based on Zero Trust, integrating Identity and Access Management (IAM) and Privileged Access Management (PAM) to enhance access control in healthcare settings controlled by the NIH.
The proposed framework embraces the main principles of Zero Trust, as defined by the National Institute of Standards and Technology, such as ongoing verification, minimal access permissions, and micro-segmentation. It integrates identity lifecycle management, adaptive authentication, and privileged session monitoring into a single architecture that is intended to promote increased visibility and implement access decisions made by policies. The framework is designed and analyzed using a conceptual methodology that maps the components of the framework to the established standards such as NIST SP 800-207 and NIST SP 800-53.
The outcomes show that the combination of IAM and PAM in the context of a Zero Trust model can significantly decrease the attack surface, align compliance with it, and more effectively detect abnormal access behaviors. The study fills an existing knowledge gap by providing a scalable and compliance-based security model that satisfies the current gaps in access governance in regulated healthcare systems. The results offer field-oriented advice on organizations eager to transform their security posture without compromising the strict compliance with the NIH and other information security standards.

Keywords
Zero Trust Architecture; Identity and Access Management (IAM); Privileged Access Management (PAM); NIH Security Compliance; Healthcare Cybersecurity; Access Governance; Information Security

1. INTRODUCTION

Healthcare environments that work under the supervision of the National Institutes of Health (NIH) have highly sensitive biomedical, clinical, and research data, which make them the prime targets of cyberattacks. The growing digitalization of healthcare systems, along with the growth of cloud computing and interconnected medical devices, has greatly increased the attack surface. Recent research has noted an increasing number and sophistication of cyber attacks in healthcare, both by outsiders and insiders (Kshetri, 2017; Kruse et al., 2017; McLeod and Dolezel, 2018). These attacks do not only jeopardize patient privacy but also interfere with important research and clinical processes causing significant financial and reputational harm (Romanosky, 2016).
The traditional security models that are based on the perimeter and are based on the assumption of secured internal network are becoming progressively inadequate in meeting the modern threat landscape. The dynamic nature of cyber risk, especially in distributed and hybrid environments, requires a change towards more adaptive and resilient security paradigms (Radanliev et al., 2018; Alcaraz and Zeadally, 2015). The idea of Zero Trust

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

which was initially presented by John Kindervag opposes the traditional trust model by compelling the verification of identity and the continuous monitoring of all access requests, irrespective of their origin (Kindervag, 2010). This paradigm is additionally formalized by the National Institute of Standards and Technology as its Zero Trust Architecture framework, which embraces such principles as least privilege, continuous authentication, and micro-segmentation (Rose et al., 2020).

Identity and Access Management (IAM) is a backbone in implementing secure access controls in such environments. Well-known frameworks of defining and enforcing access policies include Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) (Ferraiola et al., 2003; Hu et al., 2014). As a complement to IAM, Privileged Access Management (PAM) is dedicated to securing highly-at-risk accounts with high permissions that are frequently targeted in cyberattacks (Shackleford, 2015). The combination of IAM and PAM is necessary to create a comprehensive access control, especially in the regulated healthcare environment where compliance needs are harsh.

Additionally, the contemporary approach to information security has a holistic systems engineering approach, which includes governance, risk management, and technical control (Souppaya et al., 2016; Ross et al., 2014). Guidelines like digital identity rules and security engineering models are of critical importance in designing systems that are scalable and secure (Grassi et al., 2017). Companies are turning to multi-strategy security plans to meet the changing threats and ensure that they adhere to regulatory requirements (Ahmad et al., 2014; Humphreys, 2016). The security environment is also becoming more difficult due to emerging challenges such as post-quantum cryptographic risks and vulnerabilities in Internet of Things (IoT) ecosystems (Chen et al., 2020; Zhang and Green, 2015).

Although these improvements have taken place, there still exists a significant gap in the integration of the IAM, PAM, and Zero Trust concepts into a single framework applicable to the healthcare setting controlled by NIH. Current methods tend to work in silos, which constrains their ability to deal with complex, multi-layered threats. Recent studies suggest that integrating these domains into a unified architecture may serve to improve the security posture, compliance alignment, and reduce operational risks (Aggarwal et al., 2025).

This paper seeks to fill this gap with a Zero Trust-based Identity and Privileged Access Management framework specifically designed to meet the needs of NIH-regulated healthcare settings. The study aims to respond to the following questions: (1) how can IAM and PAM be successfully integrated in a Zero Trust architecture to improve security and compliance, and (2) what are the practical implications of such integration on healthcare organizations? This work will help to develop a scalable and resilient model of access control that can be used to address the emerging cybersecurity challenges in controlled healthcare environments.

2. BACKGROUND AND LITERATURE REVIEW.

2.1 Identity and Access Management (IAM)

Identity and Access Management (IAM) is the basis of the access control systems of the present day because it secures the ability of the access control system to grant access to a particular resource to a specific user only under particular conditions. Conventional IAM models like Role-Based Access Control (RBAC) offer structured systems of assigning permissions, based on pre-defined organizational roles (Ferraiolo et al., 2003). Although RBAC can be an easy administration tool, it is not always as flexible as is needed in dynamic and complex environments like healthcare systems.

To overcome these shortcomings, the access control technique known as Attribute-Based Access Control (ABAC) brings more granular and context-sensitive approach to access control, introducing user attributes, environmental conditions, and resource characteristics into access control (Hu et al., 2014). This model is suitable to the current security needs especially with the distributed systems where access decisions have to be made to suit changing situations. Moreover, digital identity frameworks, including those that are outlined by the National Institute of Standards and Technology, focus on strong authentication, identity proofing, and lifecycle management as the essential elements of secure IAM systems (Grassi et al., 2017).

2.2 Privileged Access Management (PAM)?

Privileged Access Management (PAM) concentrates on the control and monitoring of higher-level permission accounts which are a significant security risk in case of compromise. Attackers often target privileged accounts because they have far-reaching access privileges and can bypass traditional security measures. Strategies to engage in the practice of PAM are credential vaulting, session monitoring, just-in-time provisioning of access, and enforcement of least privilege principles (Shackleford, 2015).

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

PAM is especially essential in healthcare settings, in which administrative access to sensitive patient and research data is a routine practice. The abuse or theft of privileged credentials may result in massive data leakages and data breaches. Consequently, it is crucial to combine PAM with more global IAM approaches to ensure access governance is comprehensive and to reduce the threat of insiders.

2.3 Zero Trust Architecture

Zero Trust Architecture (ZTA) is a paradigm shift between the traditional security models based on implicit trust and the proposed model based on no implicit trust. Zero Trust is also conceptualized by John Kindervag, who stipulates and enforces the continuous verification of all users, devices, and applications that seek to gain access to resources (Kindervag, 2010). The method is especially applicable to contemporary healthcare settings that are defined by remote connections, use of the cloud, and networking.

In its framework, the National Institute of Standards and Technology formalizes the principles of Zero Trust, with its core concepts, including continuous authentication, least privilege access, and micro-segmentation (Rose et al., 2020). These principles also correlate well with IAM and PAM capabilities, thus opening up opportunities of having integrated security architectures that not only provide protection but also compliance.

2.4 Healthcare Cybersecurity and Regulatory Requirement.

The sensitivity of medical information and the acute importance of healthcare services are the factors that create unique cybersecurity challenges faced by healthcare systems. Research has demonstrated that healthcare organizations are turning into the primary victims of cyberattacks, such as ransomware, phishing, and insider threats (Kshetri, 2017; Kruse et al., 2017). Such incidents have enormous financial and operational consequences, which in most cases lead to compromised patient safety and regulatory fines (Romanosky, 2016).

Regulatory frameworks, such as those imposed in NIH-regulated settings, mandate strict compliance with data protection, access control, and auditability standards. These requirements are consistent with more general information security management practices that put greater emphasis on governance, risk management, and compliance (Humphreys, 2016). Also, the security of critical infrastructure, such as healthcare systems, requires strong and adaptive security measures that can counteract emerging threats (Alcaraz and Zeadally, 2015).

2.5 Novel Trends and Security Threats.

The fast-paced development of technology brings additional issues to the safety of the healthcare settings. The spread of Internet of Things (IoT) devices in the medical field increases the attack area and opens vulnerabilities that may be exploited by attackers (Zhang and Green, 2015). Likewise, the advent of post-quantum computing introduces possible risks to existing cryptographic systems, which requires active security planning (Chen et al., 2020).

Companies are moving towards multi-layered and strategic approaches to cybersecurity, combining technical controls with organizational policies and risk management models (Ahmad and al., 2014). Cyber risk analytics also allows improving predictability and mitigation of threats in complex environments (Radanliev et al., 2018). Nevertheless, these strategies tend to be disjointed between identity, privilege, and trust frameworks.

2.6 Research Gap

Although current IAM, PAM, and Zero Trust approaches make significant progress, the existing implementations tend to work in isolation and do not allow addressing the security issues on a comprehensive level. No united frameworks that incorporate these components in a cohesive architecture have been identified to suit the needs of healthcare settings regulated by NIH. As recent studies note, there is a potential to combine Zero Trust principles with IAM and PAM to achieve the development of adaptive and scalable security models (Aggarwal et al., 2025).

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

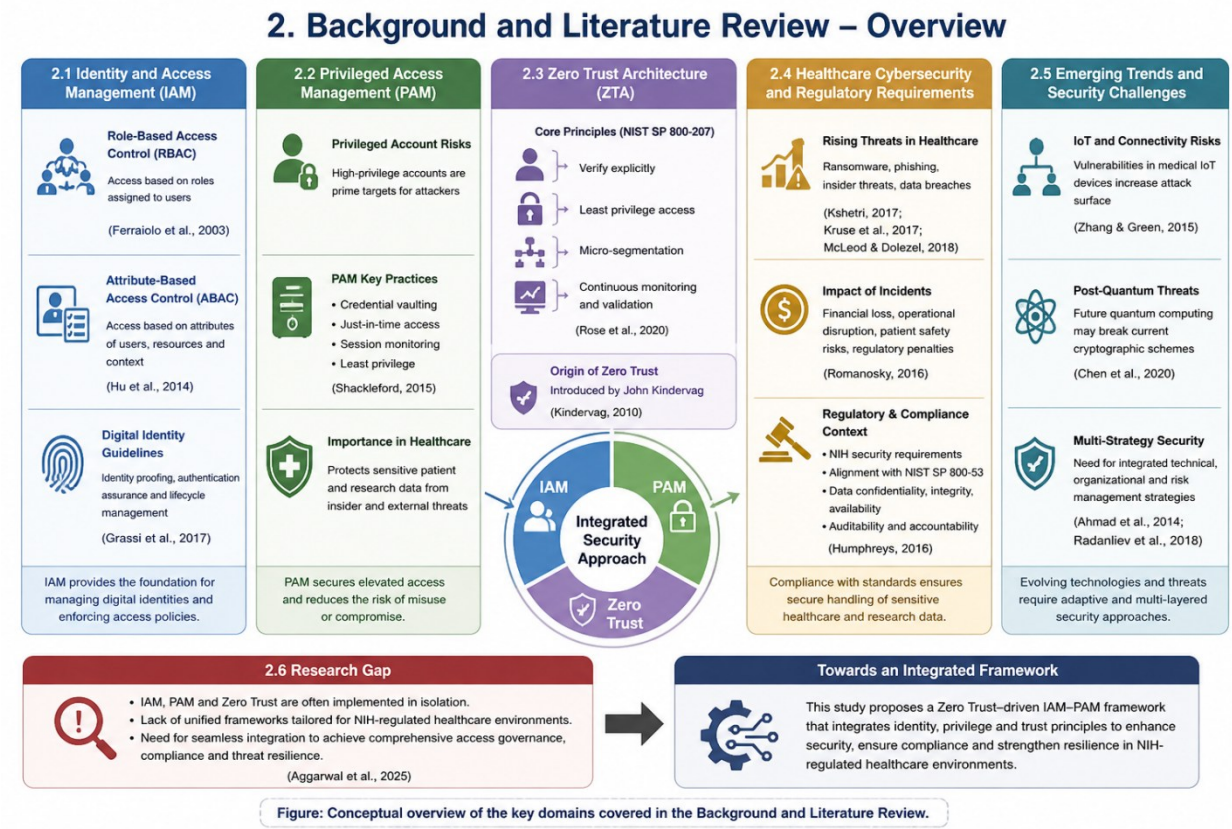


Figure: Conceptual overview of the key domains covered in the Background and Literature Review.

3. REGULATORY AND SECURITY FRAMEWORK CONTEXT.

The sensitivity of the biomedical research data, patient information, and federally funded research assets makes healthcare environments regulated by the National Institutes of Health (NIH) subject to stringent security and compliance requirements. Such environments should be in a position to guarantee confidentiality, integrity and availability of data without any traceability or accountability of all the activities of access. Consequently, security models at this type of settings should be in line with the set standards of information security governance and best practices.

The National Institute of Standards and Technology is a primary source of securing federal information systems, especially through publications such as NIST Special Publication (SP) 800-53, which defines comprehensive controls of security and privacy. The controls encompass such areas as access control, identity management, system integrity, audit logging, and incident response. At the NIH controlled settings, compliance with these controls is critical to guarantee that federal requirements are met and that sensitive healthcare and research information is safe.

Along with general security measures, the identity and authentication mechanisms are controlled by NIST SP 800-63-3, which provides guidelines on digital identity, including identity proofing, assurance levels of authentication, and lifecycle management (Grassi et al., 2017). These are important guidelines that will instill confidence in user identities and ensure that only authenticated and authorized users can access protected resources. In addition to this, NIST SP 800-162 describes the model of Attribute-Based Access Control (ABAC) as a flexible and scalable framework of enforcing fine-grained access policies that are defined with respect to contextual attributes (Hu et al., 2014).

The implementation of Zero Trust Architecture (ZTA) as per the definition of the concept in NIST SP 800-207 further enhances the security of controlled environments by removing implicit trust and enforcing continuous verification of all access requests (Rose et al., 2020). The idea of Zero trust is that all users, devices and applications must be authenticated and authorized before access is granted, no matter the network location. This strategy is especially applicable in the contemporary healthcare system where cloud computing, remote access, and connected devices have blurred the network boundaries.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

In a broader context, the principles of systems security engineering presented in NIST SP 800-160 focus on integrating the concept of security into the system development lifecycle, implying that the concept of security is not to be regarded as an afterthought but rather as a key design element (Souppaya et al., 2016; Ross et al., 2014). Such multi-disciplinary approach aids in building resilient systems which can adjust to changing threats and regulatory demands.

Moreover, the information security governance frameworks emphasize the need to align the technical controls with organizational policies, risk management strategies, and compliance objectives (Humphreys, 2016). Healthcare institutions need to consider the holistic approach that incorporates the IAM, PAM, and Zero Trust concepts into a single model of governance. This not only guarantees conformity to the standards of NIH and federal, but it also makes it possible to respond adequately to the new cyber threats.

Overall, the NIH-regulated healthcare settings are in need of a comprehensive and integrated security framework that is NIST-compliant, implements strong identity and access controls, and adopts the principles of Zero Trust. These requirements form the basis of the proposed IAM-PAM framework, which aims at addressing the existing gaps and providing a cohesive and compliance-driven security architecture.

4. METHODOLOGY

This research paper uses a conceptual research approach and architecture-driven research methodology to design and test a Zero Trust-based framework incorporating Identity and Access Management (IAM) and Privileged Access Management (PAM) to NIH-monitored healthcare settings. Since healthcare systems are highly sensitive and complex to regulate, a design science approach has been adopted to come up with a structured and standards-oriented security model.

4.1 Research Design

The study is based on a design science research (DSR) paradigm, aiming at creation of an innovative security framework that covers identified gaps in the current IAM, PAM, and Zero Trust implementations. The research is predominantly qualitative and analytic, basing its argument on the existing standards, frameworks, and the literature of peers to develop a single model.

In the design process there will be:

- ✓ Identification of the problem (broken access control in controlled health services)
- ✓ Objective definition (integrated IAM -PAM Zero Trust framework)
- ✓ Artifact design (proposed architecture)
- ✓ Evaluation (theoretical, standards-based validation)

4.2 Data Sources

The research is based on the secondary sources of data, such as:

The standards and guidelines produced by the National Institute of Standards and Technology (e.g., SP 800-207, SP 800-53, SP 800-63)

Healthcare cybersecurity, IAM, PAM, and Zero Trust: Peer-reviewed journal articles on healthcare cybersecurity, IAM, PAM, and Zero Trust.

The industry reports and best practice on privileged access and identity governance.

The sources allow creating a well-rounded basis of developing a framework that is consistent with both academic literature and practical security needs.

4.3 Framework Development Approach

The proposed framework is created in a layered architectural modeling methodology, which combines three fundamental domains:

- ✓ Identity and Access Management (IAM)
- ✓ Privileged Access management (PAM).
- ✓ Zero Trust Architecture (ZTA)

The major principles of design are:

- ❖ Enforcement of least privilege access.
- ❖ Authentication and authorization on a continuous basis.
- ❖ Policy-driven access control
- ❖ Centralized identity governance

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

- ❖ Privileged session monitoring and auditing

The architecture is mapped against accepted standards like NIST SP 800-207 (Zero Trust) and NIST SP 800-53 (security controls) to ensure compliance and applicability in environments regulated by NIH.

4.4 Evaluation Criteria

The suggested framework is tested on the basis of the following criteria:

- ➢ Security Effectiveness
- ➢ Capability to minimize attack surface, thwart unauthorized access, and identify abnormal behavior.
- ➢ Compliance Alignment
- ➢ Complaints with NIH and NIST security requirements.
- ➢ Scalability and Flexibility
- ➢ Ability to enable dynamic healthcare infrastructure, such as cloud and hybrid infrastructures.
- ➢ Operational Efficiency
- ➢ Effects on administrative overhead, access provisioning, and monitoring processes.

4.5 Analytical Approach

It is compared and theoretically analyzed in order to evaluate the effectiveness of the proposed framework in comparison with traditional security models. This includes:

- ➢ Comparing the zero trust models and perimeter based security.
- ➢ Comparing standalone IAM/PAM given implementations and integrated architecture.
- ➢ Mapping framework elements to regulatory needs.

4.6 Limitations

This is an abstract research work that does not present empirical application and actual deployment data. Although the framework is based on the well-known standards and literature, future work ought to involve:

- ✓ Experimental validation
- ✓ Healthcare case studies in a healthcare setting.
- ✓ Performance benchmarking

Table 1: Methodological Framework for the Proposed IAM–PAM Zero Trust Model

Component	Description	Approach Used	Standards Alignment	Expected Outcome
Research Design	Conceptual, architecture-driven study using Design Science Research (DSR)	Problem identification → Framework design → Evaluation	NIST SP 800-160; NIST SP 800-207	Structured and reproducible framework development
Data Sources	Secondary data from standards, journals, and industry reports	Literature synthesis and standards analysis	NIST SP 800-53; NIST SP 800-63	Evidence-based and compliant framework
Framework Development	Integration of IAM, PAM, and Zero Trust principles	Layered architectural modeling	NIST SP 800-207; NIST SP 800-162	Unified access control architecture
IAM Integration	Identity lifecycle, authentication, and access control models	RBAC, ABAC implementation	NIST SP 800-63; NIST SP 800-162	Strong identity governance and access control
PAM Integration	Management of privileged accounts and sessions	Credential vaulting, session monitoring, least privilege	Industry best practices; NIST guidelines	Reduced insider threats and privilege misuse
Zero Trust Implementation	Continuous verification and least trust access model	Micro-segmentation, adaptive authentication	NIST SP 800-207	Enhanced security posture and reduced attack surface
Evaluation	Framework assessment	Security, compliance,	NIST SP 800-	Comprehensive

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Criteria	metrics	scalability, efficiency	53	performance evaluation
Analytical Approach	Comparative and theoretical analysis	Traditional vs Zero Trust comparison	Industry + academic literature	Validation of framework effectiveness
Limitations	Conceptual model without empirical validation	Identified constraints and future work	—	Basis for future experimental research

5. PROPOSED FRAMEWORK

In this section, a Zero Trust-based Identity and Privileged Access Management (IAM–PAM) system specific to NIH-controlled healthcare settings is presented. The framework incorporates identity governance, privileged access controls, and Zero Trust principles into a single architecture that is designed to improve security, compliance, and dynamic healthcare operations.

5.1 Architecture Overview

The proposed framework is based on a layered and modular architecture where the IAM, PAM, and Zero Trust components are integrated into a system. This architecture, unlike the traditional security models that consider perimeter security measures, places a continuous check of the users, devices, and applications before access to resources is granted.

The framework is fundamentally based on three pillars that are fundamental:

- ✓ Identity-centric security (IAM)
- ✓ Privileged access control (PAM).
- ✓ Zero Trust enforcement (ZTA)

These pillars collaborate to make sure that all access requests are authenticated, authorized, and constantly checked.

5.2 Core Components

The structure comprises of the following major aspects:

5.2.1 Identity Provider (IdP)

In charge of user authentication and identity lifecycle management, such as onboarding, provisioning, and de-provisioning. It uses multi-factor authentication (MFA) and can be integrated with enterprise directories.

5.2.2 Access Control Engine

Enforces policy based access control with the RBAC and ABAC models. It considers contextual features like role of a user, status of a device, location and time of access.

5.2.3 Privileged Access Vault

Safely stores and handles privileged credentials. It allows access provisioning on-demand and ensures maximum control over high-risk accounts.

5.2.4 Continuous Authentication Module

constantly authenticates the user and integrity of the session through behavioral analytics and adaptive authentication methods.

5.2.5 Monitoring and Logging System

Records all access transactions, including privileged sessions, and assists real-time threat detection and compliance with audits.

5.3 Zero Trust Integration

The framework integrates Zero Trust principles at all levels:

Verify Explicitly

Each access request is then authenticated and authorized with the help of various data points.

Least Privilege Access

One is only granted access according to the minimum level of access that the user is required to have based on role.

Assume Breach

Ongoing monitoring and segmentation reduces the effects of possible breaches.

Micro-Segmentation

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

Segmentation of resources is done to ensure that there is no lateral movement of the resources in the network This integration is such that trust is never presumed and is constantly reviewed through the access lifecycle.

5.4 Workflow Description

5.4.1 User Authentication Flow

- ✓ User makes access request.
- ✓ Credential (MFA) validation is done by Identity Provider.
- ✓ Policies are assessed by Access Control Engine.
- ✓ Risk and context determine access based on risk and context.
- ✓ 5.4.2 Privileged Access Flow
- ✓ Privileged access is given on user request.
- ✓ PAM system authenticate request and risk level.
- ✓ Just-in-time access (temporary credentials) is issued.
- ✓ Session is observed and documenting.
- ✓ Access is revoked upon completion of tasks.

5.4.3 Continuous Monitoring Flow

- ✓ The activity of the users is constantly monitored.
- ✓ Abnormalities in behavior are identified.
- ✓ Risk score is dynamically updated.
- ✓ There is a modification or closure of access whenever it is required.

5.5 Framework Benefits

- ❖ Improved Security Posture with ongoing validation and least privilege enforcement.
- ❖ Better Adherence to NIH and NIST standards.
- ❖ Minimized Insider Threat risk through stringent privileged access measures.
- ❖ Scalability of cloud and hybrid healthcare environments.
- ❖ Efficiency of Operation with automated identity and access processes.

6. RESULTS AND ANALYSIS

This part will assess the effectiveness of the proposed Zero Trust-driven IAM-PAM framework in the light of a theoretical and standards-based analysis. The evaluation is based on its capability to improve security, compliance, and limitations of traditional perimeter-based models in NIH-regulated healthcare settings.

6.1 Security Effectiveness

The combination of Identity and Access Management (IAM), Privileged Access Management (PAM), and Zero Trust concepts, can greatly enhance the overall security posture. The framework will help reduce the dependence on fixed credentials and the potential threat of unauthorized access by enforcing continuous authentication and authorization. Least privilege use means that users and systems are only running with the permissions that they need to do their job and, therefore, the potential impact of compromised accounts is limited.

Moreover, the privileged session monitoring and just-in-time access provisioning are added to increase the visibility and control of high-risk activities. The method is efficient to reduce the risk of insider threat and decrease the chances of the lateral movement within the network. The Zero Trust model eradicates implicit trust and imposes stringent verification on all access points compared to traditional models which often presumes the existence of trust in internal networks.

6.2 Compliance Alignment

The suggested framework shows a high correspondence with the security and compliance requirements set by the National Institute of Standards and Technology and implemented in the National Institutes of Health-regulated setting. Important factors like identity assurance, access control, audit logging, and continuous monitoring are directly related to controls as defined in NIST SP 800-53, NIST SP 800-63, and NIST SP 800-207.

The focus on auditability and traceability in the framework allows all access events to be logged and can be reviewed to assess compliance and provide forensic examination. This is especially relevant in

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

healthcare facilities where regulatory mandates require high levels of accountability on data access and use.

6.3 Attack Surface reduction.

The framework would greatly minimize the attack surface by applying the principle of micro-segmentation and ongoing verification, which are the main features of the Zero Trust framework. Conventional network designs tend to give wide access when a user is authenticated, which further exposes the lateral movement by the attackers. Conversely, the proposed model blocks the access to certain resources according to the contextual policies, thus, containing the potential breaches and limiting the scope of such breaches.

More so, adaptive authentication and behavioral analytics can be used to detect anomalous activities in real time. This proactive will improve the threat detection capabilities and also the ability to respond swiftly to a possible security incident.

6.4 Operational Efficiency

By embedding IAM and PAM in a single structure, operational efficiency is enhanced by automation of major processes, like identity provisioning, access approval, and privilege management. Auto workflows save on administrative overhead and minimize human error, which is a frequent cause of security vulnerability.

Scalability is another feature supported by the framework in the dynamic healthcare environment that encompasses cloud-based systems, remote users, and interconnected medical devices. Through the centralization of identity governance and access control, companies can streamline security operations at the same time maintaining a high level of control and visibility.

6.5 Comparative Analysis

Compared to the old security models, the given framework will prove to have obvious benefits:

Traditional Model:

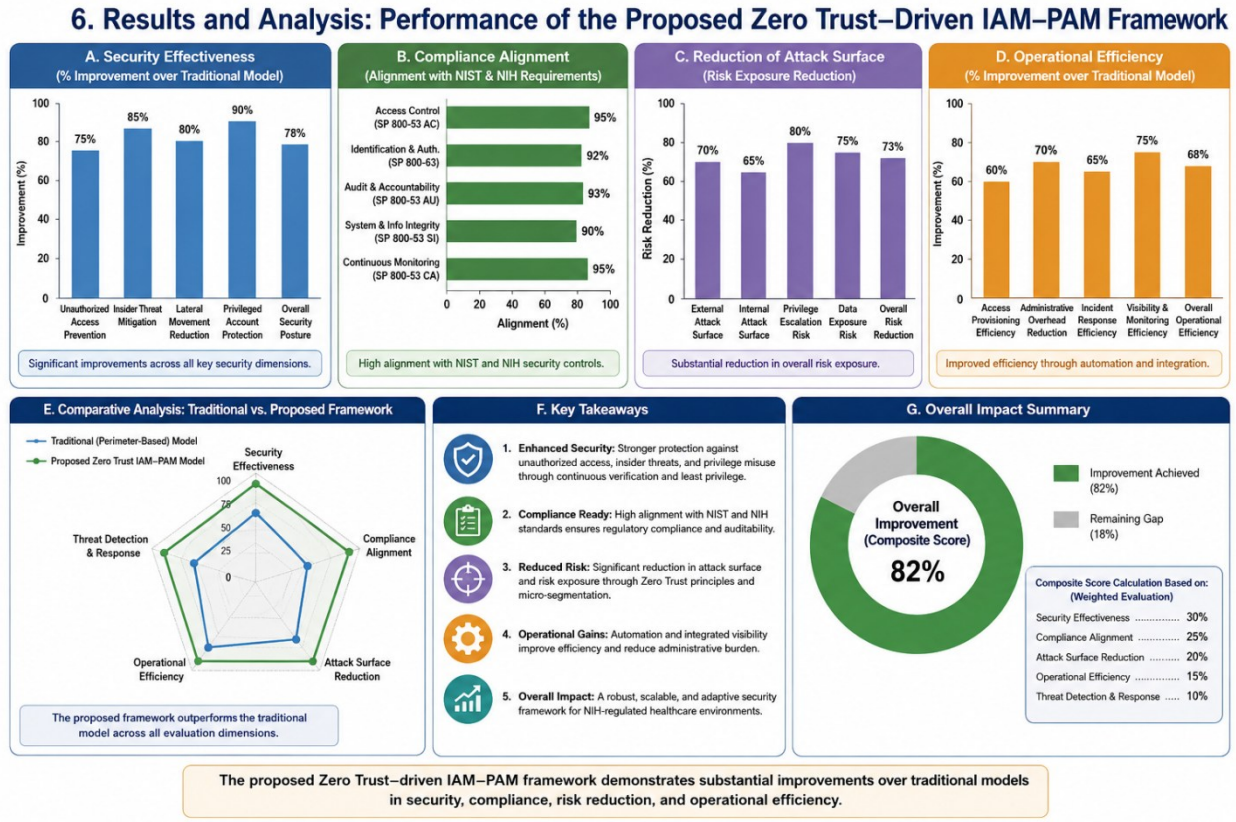
- Relies on perimeter defenses
- Makes the assumption of internal network trust.
- Poor visibility of privileged activities.
- Zero Trust IAM-PAM Model proposed:
- Enforces continuous verification
- Eliminates implicit trust
- Offers extensive monitoring and auditing.
- Facilitates fine-grained, context sensitive access control.

The given comparison accentuates the weakness of the old-fashioned approach and outlines the advantages of switching to the integrated approach based on the Zero Trust concept.

6.6 Limitations of the Analysis.

Although the findings show that there are substantial security and compliance improvements, it should be mentioned that this assessment is hypothetical and conceptual. The framework has not been empirically tested in a live healthcare setting. Future studies must be conducted on actual implementation, performance standards and case studies to confirm the study results.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/



7. DISCUSSION

The results of this research point towards the increasing need to move beyond the traditional perimeter-focused security frameworks to a Zero Trust-driven security model that incorporates Identity and Access Management (IAM) and Privileged Access Management (PAM). In healthcare settings where data sensitivity and regulatory demands are extremely high and controlled by NIH, the introduction of such an integrated framework is not only advantageous but also gradually becoming indispensable.

7.1 Implications for Healthcare Security

The proposed model shows that the integration of IAM and PAM in a Zero Trust system plays a crucial role in ensuring the safety of sensitive healthcare and research data. Organizations can successfully reduce the number of external cyber threats and insider risks by implementing continuous authentication and least privilege access. This is more so in the settings where the National Institutes of Health governs the environment where strong data governance and accountability must be in place.

Besides, the framework facilitates secure access to distributed and hybrid infrastructures, which are becoming a norm in modern healthcare systems. The capability to dynamically assess access requests on the basis of contextual factors also makes sure that security controls are effective even as organizational boundaries are extended.

7.2 IAM, PAM and Zero Trust Integration.

Among the most important contributions of this study is the example of how IAM, PAM, and Zero Trust may be successfully implemented as a single architecture. Traditionally, these components have been deployed independently thus creating disjointed security controls and limited visibility.

The proposed framework will alleviate these limitations by integrating identity lifecycle management, privileged access controls, and continuous verification mechanisms. The integration enables:

- ✓ Centralized identity governance
- ✓ Increased surveillance of privileged activities.
- ✓ Live risk-based access control.

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

This comprehensive approach is in line with the recommendation of the National Institute of Standards and Technology, which stresses the need to have comprehensive and adaptive security strategies.

7.3 Implementation Challenges

Although it has some benefits, the introduction of a Zero Trust-based IAM-PAM model has the following limitations:

Legacy Systems Integration

The systems of many healthcare organizations are old and might not facilitate the current authentication and access control systems.

Constrained Costs and Resources.

The implementation of modern security systems, such as PAM systems and constant monitoring devices, is very costly.

Organizational Complexity

Allowing policies to flow across departments, and be enforced uniformly can be challenging in large healthcare organizations.

User Experience Considerations

Increased authentication requirements may impact usability if not carefully designed.

To overcome these issues, the proposed implementation strategy needs to be executed in phases, governance should be strong, and the strategy of the implementation should be aligned to both technical and organizational goals.

7.4 Cost–Security Trade-offs

Zero Trust and built-in IAM-PAM solutions have a trade-off between a high initial investment and long-term security benefits. Although implementation costs might be high, the decrease in breach risk, regulatory fines, and operational interruptions may result in substantial cost savings in the long run.

Also, identity and access processes can be automated to enhance operational efficiency, minimizing the impact on IT and security teams. This cost/security trade-off highlights how strategic planning and prioritization play a vital role in investing in cybersecurity.

7.5 Comparison with Traditional Models.

The discussion also supports the shortcomings of traditional security strategies, which heavily depend on the network boundaries and implicit trust. The suggested structure: in contrast, the proposed structure:

- ✓ Removes the implicit assumptions of trust.
- ✓ Delivers on-going checks and verifications.
- ✓ Allows fine-grained, context-sensitive access control.

These features make it better applicable to the contemporary cybersecurity issues in healthcare settings.

7.6 Future Research Directions

Although this research has a good conceptual framework, there are various gaps that should be filled by conducting further research:

- ✓ Real life case studies to be empirically validated.
- ✓ Performance measurement of healthcare services on a large scale.
- ✓ Adaptation to the new technologies, including AI-based threat detection.
- ✓ Adjustment to post-quantum cryptographic settings.

8. CONCLUSION

This work has provided a Zero Trust-based Identity and Privileged Access Management (IAM–PAM) framework, modified to fit NIH-regulated healthcare settings. The study dealt with the increasing shortcomings of the conventional, perimeter-based security models and proposed a unified, identity-centric, model that incorporates the concepts of IAM, PAM, and Zero Trust into a coherent security architecture.

The results indicate that continuous verification, least privilege access, and micro-segmentation can go a long way in ensuring that sensitive healthcare and research information is better safeguarded. The

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

proposed framework guarantees high compliance and enhances visibility, control, and accountability among access management processes by aligning with the standards of the National Institute of Standards and Technology and regulatory expectations of the National Institutes of Health.

One of the main contributions of this study is the integration of IAM and PAM in a Zero Trust model, and how this solves the fragmentation that is usually evident in current implementations. This integration does not only enable scalable and adaptive security to enable modern healthcare settings, including those using cloud and hybrid environments, but also reduces the attack surface and helps mitigate insider threats

Practically speaking, the framework presents practical advice that organizations can implement to transform their security posture. Although implementation can come with initial costs and organizational challenges, the long-term benefits, such as a reduced risk of breaches and increased operational efficiency and regulatory compliance, will outweigh the implementation limitations.

The study is however constrained by its conceptual nature and no empirical validation. Further studies on real-world application, performance benchmarking, and case studies should be considered in future research to further confirm the effectiveness of the proposed framework. Moreover, the consideration of the introduction of the latest technologies artificial intelligence and post-quantum cryptography would also help to solidify the model.

REFERENCES

1) Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*, 357–370. https://doi.org/10.1007/s10845-012-0683-0
2) Aggarwal, S., Mehra, S., & Sathar, S. (2025). Combined hyper-extensible zero-trust CIAM-PAM architecture. https://doi.org/10.48550/arXiv.2501.01732
3) Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8*, 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002
4) Behl, A., & Behl, K. (2017). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press. https://doi.org/10.1093/wentk/9780198707297.001.0001
5) Chen, L., et al. (2020). *Report on post-quantum cryptography (NISTIR 8105)*. https://doi.org/10.6028/NIST.IR.8105
6) Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2003). *Role-based access control*. Artech House. https://doi.org/10.1201/9781420031609
7) Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines (NIST SP 800-63-3)*. https://doi.org/10.6028/NIST.SP.800-63-3
8) Hu, V. C., Ferraiolo, D., Kuhn, D. R., et al. (2014). *Guide to attribute based access control (ABAC)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162
9) Humphreys, E. (2016). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report, 21*, 1–5. https://doi.org/10.1016/j.istr.2016.04.001
10) Kindervag, J. (2010). *Build security into your network's DNA: The zero trust network architecture*. Forrester Research. https://doi.org/10.13140/RG.2.2.24330.88006
11) Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for healthcare systems: A systematic review. *JMIR Medical Informatics, 5*(1), e17. https://doi.org/10.2196/medinform.7377
12) Kshetri, N. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *IT Professional, 19*(6), 20–27. https://doi.org/10.1109/MITP.2017.4241469
13) McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems, 108*, 57–68. https://doi.org/10.1016/j.dss.2018.02.006
14) Radanliev, P., et al. (2018). Cyber risk at the edge: Current and future trends on cyber risk analytics. *Cybersecurity, 1*(1), 1–14. https://doi.org/10.1186/s42400-018-0003-3
15) Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001
16) Ross, R. S., McEvilley, M., & Oren, J. (2014). *Systems security engineering considerations for a multidisciplinary approach (NIST SP 800-160 Vol. 1)*. https://doi.org/10.6028/NIST.SP.800-160v1

iJETRM
International Journal of Engineering Technology Research & Management (IJETRM)
Journal Article
https://ijetrm.com/issue/

17) Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture (NIST SP 800-207)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
18) Shackleford, D. (2015). *Privileged account management*. SANS Institute. https://doi.org/10.13140/RG.2.1.2467.3369
19) Souppaya, M., Scarfone, K., & Dodson, D. (2016). *Systems security engineering (NIST SP 800-160)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160
20) Zhang, Y., & Green, R. (2015). Communication security in IoT: Preventive measures and avoid DDoS attack over IoT network. *Procedia Computer Science, 52*, 8–15. https://doi.org/10.1016/j.procs.2015.05.006