Securing Non-Human Identities (NHIs) in Cloud-Native Healthcare Systems

Anjan Gundaboina

Senior DevsecOps and Cloud Architect
USA.

anjankumar.247@gmail.com

Abstract:
In the recent past, industry-wise virtualization changes and alterations to cloud computing have provided better adaptability, care integration, capabilities, and remote care services. However, these advances have provided them with new problems, specifically regarding cybersecurity, especially in the case of NHI medical devices, services, applications, and agents that act freely within these environments. NHIs communicate within different cloud settings, sharing and retrieving patient information, which is commonly done with little to no supervision. The development of the Internet of Medical Things and the microservice architecture in the health sector has upped the risks needed to secure NHI. This paper examines a holistic approach to protecting NHIs in cloud-native healthcare ecosystems. First, we discuss the prevailing architectural strategies in such systems and then describe the issues particular to NHIs. We then review research and guidelines on managing NHI and Cloud security from literatures and standards. Our proposed approach comes with a layered identity security architecture that follows the principles of Zero Trust Architecture (ZTA), non-human identity governance, human behavior analysis, and identity-based access control. We evaluate the developed approach using a realistic imitative hospital network comprising various IoMT devices and cloud services. Concerning the findings from the network traffic analysis, the results depicted have highlighted the aspects of anomaly detection, attack risks, and the relative HIPAA and NIST cybersecurity frameworks compliance. This suggests the need to redesign identity in healthcare to include other layers so as to realize the health system's integrity and patient safety.

Keywords: Non-Human Identity (NHI), Cloud-Native Healthcare, Zero Trust Architecture, Behavioral Analytics, Identity and Access Management (IAM).

1. INTRODUCTION

Microservices, containers and distributed systems are at the center of the cloud-native systems, which support highly available and scalable architectures required in the healthcare domain's IT systems. [1-4] As such, identity shifted from purely patient and provider orientation to comprising medical devices, software agents and virtual machines, also referred to as Non-Human Identities (NHIs).

1.1. Role of NHIs in Healthcare

- **Continuous Monitoring via IoMT Sensors:** NHIs like the IoMT sensors facilitate the constant monitoring of patients because they are a type of smart connected device. They include devices that monitor the patients' rate of heartbeat, their oxygen needs, and the glucose level in their blood continuously to facilitate effective healthcare and instant medical care. Their capability of working on their own without the supervision of the human being depicts them as reliable and consistent sources of vital health information.
- **Data Preprocessing Through Edge Gateways:** Its NHIs are edge gateways that preprocess data closer to the source of the data, location usually close to patient devices. Because data filtering, aggregation, and analysis are done locally at these gateways, they cut latency, minimize bandwidth usage, and decentralize the workload from central systems. This localized intelligence only forwards credible or out-of-the-ordinary data to the cloud making the system fast and more efficient.

- **Autonomous Diagnostics Using AI Agents:** There are self-driven NHIs that diagnose health conditions based on structured data, images, or sensors. These agents use algorithms in machine learning to find out particular conditions such as arrhythmias or early-stage cancer and are often quicker than the human system. These are to provide consultation for decision-making processes, enhance efficiency in diagnostic procedures, and enhance the workflow's efficiency.
- **Secure Communication Through APIs and Services:** NHIs' APIs and service endpoints create the necessary link to secure and interoperable communications between healthcare systems. They enable the securing of the transfer of information among such things as EHR systems, mobile applications, and medical devices with encryption and identity-based access control. These are the essential services of healthcare networks; the distribution of medical data is secure due to compliance with regulations regarding privacy.

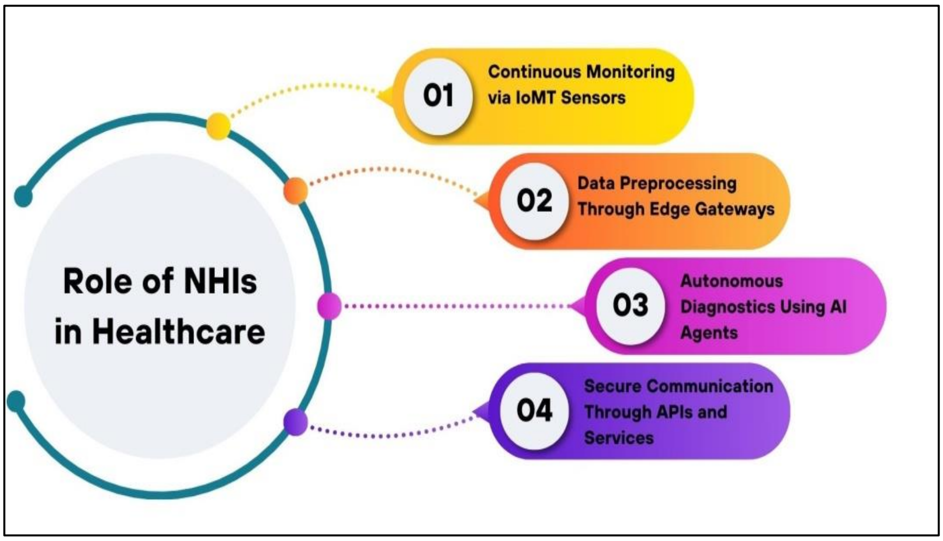
Role of NHIs in Healthcare
01 Continuous Monitoring via IoMT Sensors
02 Data Preprocessing Through Edge Gateways
03 Autonomous Diagnostics Using AI Agents
04 Secure Communication Through APIs and Services

Fig 1. Role of NHIs in Healthcare

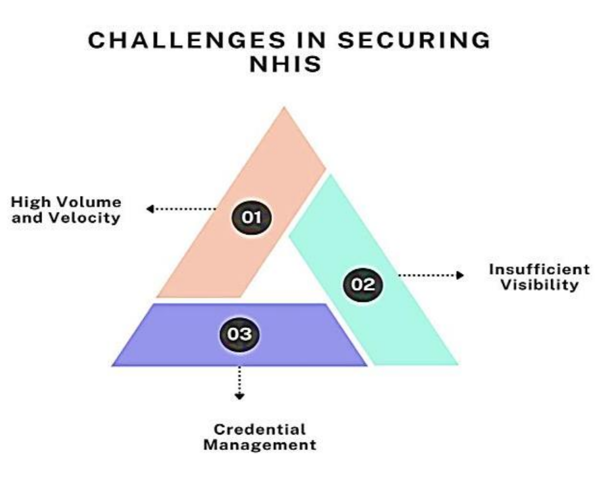
CHALLENGES IN SECURING NHIS
01 High Volume and Velocity
02 Insufficient Visibility
03 Credential Management

Fig 2. Challenges in Securing NHIs

1.2. Challenges in Securing NHIs

- **High Volume and Velocity:** NHIs are implemented on a large scale in various contexts of the health sector, such as hospitals, laboratories, and telemedicine. Some run in short-lived contexts like containers or serverless functions, where identities are short-lived and may change within a short time. This is because their volume and velocity are high, and each NHI needs to be authenticated and managed consistently to enhance security and minimize possible blind spots and other illicit activities.
- **Insufficient Visibility:** Adopting traditional IAM solutions for semantically enhancing the translated code is inefficient. These solutions are developed for human users and user access control and,

therefore, cannot address the minute differences and high level of detail of m2m interactions. As the NHI engage in APIs, services, or network protocol interactions, it is difficult to ensure that they indicate compliance with upheld policies, identify suspicious activity, or even track malicious activities. This weak link is detrimental to security measures and complicates the investigation process in the case of a breach.

- **Credential Management:** Another critical factor that any organization faces in securing NHIs is the issue of dealing with the credentials of the NHI. Some real-world examples include hardcoded secrets, expired tokens, misconfigured access keys, and many more. These are the kinds of risks that are often perhaps exploited to provide unauthorized access to information or substances within an organization. If credential provisioning, rotation and revocation are not done automates, the NHIs risk having a leakage or privilege escalation attack.

1.3. Securing Non-Human Identities (NHIs) in Cloud-Native Healthcare Systems

Assuring Non-Human Identities (NHIs) in cloud-native healthcare systems is emerging as a critical challenge since modern healthcare is shifting to interconnected and self-operating devices, services, and intelligent agents. LoT assets like IoMT sensors, APIs, service accounts, containers, and AI algorithms are keys to the functionality of modern healthcare organizations, and their security requirements are quite different from those of traditional end-users. In contrast, and more importantly, the NHI user population is significantly different, consisting of less stable credentials and roles, remaining in highly dynamic and especially ‘ephemeral’ environments and often self-provision based on system load. This complicates the creation, evaluation, or even withdrawal of these guardian structures necessary for the healthy growth of a secure operational environment. [5,6] In cloud-native architectures, hosts can be contained or micro-serviced, located in containers that can come up and down frequently and may not have permanent names. This makes it impossible for conventional security models to monitor and regulate their activities compared to cases of traditional cyber threats. Also, when one machine writes to another such as an AI diagnostic tool pulling information from a patient’s database through an Application Program Interface or API, the traffic is not easily discernible if not for logging mechanisms. As it has been observed, conventional IAM tools cannot identify cases of misuse or anomalous behaviour, if any, in these interactions. The absence of real-time behavioral analysis in most systems worsens the situation; hackers might be able to breach the system without being noticed. Credential management is another issue added to it. A coded secret, tokens or API are well-known risk causes when they are hardcoded or shared and stored unnecessarily long. If the NHIs are not issued, renewed and revoked automatically, it becomes a clothesline security issue. To mitigate these threats, a Zero Trust Architecture (ZTA) framework is required to oversee and ensure continuous verification, just-in-time access, and use-of-function access control. These strategies and sophisticated and constant monitoring and behavioural analysis offer a framework for protecting NHIs in the challenging and regulatory-compliant environment of CN-sharing arrangements for healthcare services.

2. LITERATURE SURVEY

2.1. Existing NHI Security Models

The current body of work concerning Networked Healthcare Infrastructure (NHI) security trends has dealt with different identity and access management aspects. and have stressed the fact of machine identity, especially with regard to the certification of devices with mutual and continuous authentications throughout the healthcare network. This reduces the chances of making mistakes and increases company operations efficiency. In the same context, address security in the Internet of Medical Things (IoMT) and create a new optimized lightweight encryption model for constrained medical sensors. The solution can successfully encrypt the data and does not affect its security on a performance level. [7-10] contribute to cloud IAM by proposing a role-based access control to the API in the hybrid paradigm of healthcare. This improves the level of accessibility control of users and, at the same time, ensures compatibility across the cloud services.

2.2. Gaps in Current Literature

However, various challenges have remained unsolved to date in the current NHI security architectures. There is only a limited reflection of a comprehensive identity model that can embrace both on-premises and cloud environments. It hurts most present-day models, which target segments individually and leave the healthcare structures open to fragmented security stances. However, the major drawback is the absence of a link to the behavioral analytics. With reference to the behavioral baselining, actions by users or a particular machine that may not be normal may easily go unnoticed, posing more threats of getting breached. Additionally, the subject of the research – Zero Trust Architecture (ZTA) has not been adequately customized or implemented for healthcare systems that require a combination of several models and present various compliance and logistical requirements. Such gaps explain why a more holistic and hierarchical security approach is required in the healthcare system.

2.3. Standards and Regulations

Several standards and regulations are followed in the deployment of NHI systems securely. The 'NIST SP 800-207' describes the Zero Trust Architecture and seeks to eliminate trust and implicit trust at every stage. The three-fold purpose is to help fill such needs and inform the means for remediating novel security postures in multidimensional landscapes of operations such as healthcare. Specifically, as per the HIPAA Security Rule, ePHI must be protected regarding confidentiality, integrity, and availability. Patients need to be assured that their data is respected, which is why compliance is often legal but also necessary. The OWASP IoT Top 10 highlights common vulnerabilities in IoMT devices, such as insecure network services and insufficient authentication mechanisms. These guidelines give guidelines to developers and IT administrators to safeguard from risks associated with connected healthcare systems.

2.4. Key Takeaways

From the literature and study of the regulations, it is clear that there is a need to have a single identity framework when addressing NHIs. For such a framework, it would be critical to incorporate anomaly detection based on probing machine learning models with respect to the identified suspicious behaviours to facilitate real-time detection of the behaviors. Furthermore, great distinctions must be made in the ability to apply policies due to the existing number of user roles and their permissions in healthcare contexts, allowing only the required access. Last, there is also a concept known as credential rotation, which must be integrated to only work in real-time. The time within which the credentials can be misused is also limited to improve the overall security of the systems. This paper contains the core of a strong, versatile, and sustainable healthcare security model for the future.

3. METHODOLOGY

3.1. System Architecture Overview

The approach to protect NHI is based on layering and includes patient devices, the edges, the cloud, and decision-makers. This modular design has easy scalability high responsiveness, and provides security from the design, implementation up to usage. [11-14] The following are the main elements of the architecture:

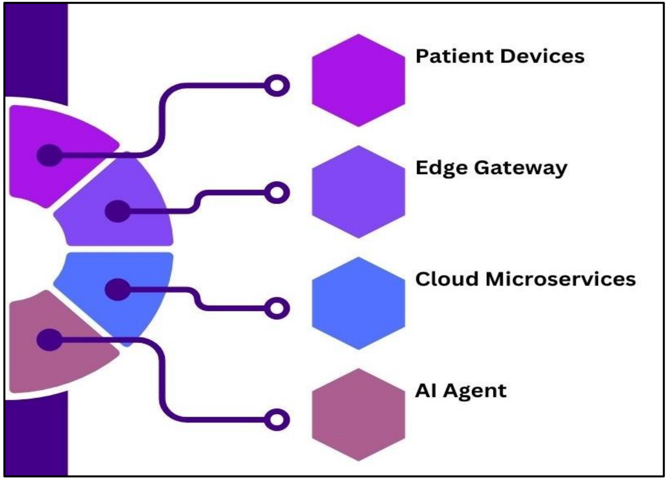

Fig 3. System Architecture Overview

- **Patient Devices:** At the user end, there are Patient devices, which are Wearable health monitors, mobile health apps and Implantable medical devices that collect important physiological data of the patient like heart rate, glucose level and blood pressure. These Internet of Medical Things (IoMT) devices have several constraints on resources while they are more vital to address security concerns since they can be attacked easily. To contain this, the authorization of data and the devices is done at the firmware level. The acquired secure data are transferred periodically to an edge processing gateway, guaranteeing the lowest latency and patients' privacy.

- **Edge Gateway:** The edge gateway acts as a bridge between patient devices and other devices in the cloud. Located nearer to the data source, it is charged with preprocessing of the data, local formatting, and normalization of the protocol. It also carries out the primary threat detection routines and implements the usage of cached credentials as a means of access control. This offloading helps lighten the cloud systems' computational load and allows real-time analysis. According to the security scope, the edge layer is key in protecting secure tunnels and device trust scores, permitting only secure data streams towards the core layer.
- **Cloud Microservices:** The cloud microservices layer provides logic and services of applications utilized for the functioning of actual healthcare treatment. It comprises reusable components like patient data storage, analysis engines, and identity management components that can function and evolve individually. All microservices communicate through APIs, and while all of them are secure and follow the Zero Trust security model, it does mean that even requests from within the same microservice are authenticated and authorized. Cloud-based IAM systems restrict the data of different populations (physicians, caregivers) for access by the relevant users whose authorization has been granted.
- **AI Agent:** The AI agent is the cognitive layer that would come into the system to introduce intelligibility and flexibility. It constantly observes the users' behavior and the system's activity to identify problem patterns, foresee threats, and indicate alterations in the policy. Providing the AI agent with training from both historical and collected data sources, it is capable of recognizing and distinguishing the examination of log-in profiles which are different from the user's normal routines, a device acting abnormally, and noncompliance with laid organizational policies which may create or signify a threat from an insider or malware. Furthermore, it helps to rotate the credentials in real-time and, change the policies and alert generations so that the system is always protective against advanced cyber threats. It helps to transform the healthcare structure of how the reactions from protective measures are managed to a proactive setting.

3.2. Layered Security Model

The Layered Security Model is meant to increase security measures of healthcare facilities' frameworks, thus incorporating several levels of security and protection. Thus, each layer performs a specific function that will give overall protection against various threats.

- **Identity Management:** The Identity Management layer, which corresponds with the layer, is responsible for providing trust anchors for machines so that the identity of any device, user, and service can be verified before being given access to the system. This layer ensures that only such devices or healthcare workers are allowed to access these data. Part of the security of Advanced Micro Devices and the generally reliable flow of information through all the levels of the infrastructure rely on certificates or cryptographic keys that guarantee the respective identities.
- **Access Governance:** This level involves the right level of access to the system by the desired users and/or devices. This is done by policy-based security, which is centered on who has the right to access certain data and when he/she has this right. RBAC or ABAC policies are implemented to restrict and enforce access, where user or device attributes or even other contexts are also considered to eliminate privilege and reduce the attack surface.
- **Monitoring & Analytics:** The Monitoring & Analytics layer declares the ongoing observation of the system actions to identify possible risks. Behavioral profiling and alerts are the primary activities in this layer, where each activity and behavior of the device are monitored for any changes. In addition, the users' habits may be mapped using machine learning techniques, meaning that any deviations can be detected in real-time, preventing any system breach.
- **Remediation:** The Remediation layer is supposed to perform fast and self-contained actions to detect a security threat. There are features for automated revocation and isolation; this helps to remove the logically compromised device, accounts, or identity from using the resources in the network to avoid furthering malicious actions. This layer also practices the cancellation of compromised credentials so that the attackers cannot continue to gain access, and hence, the system remains secure from further threats.

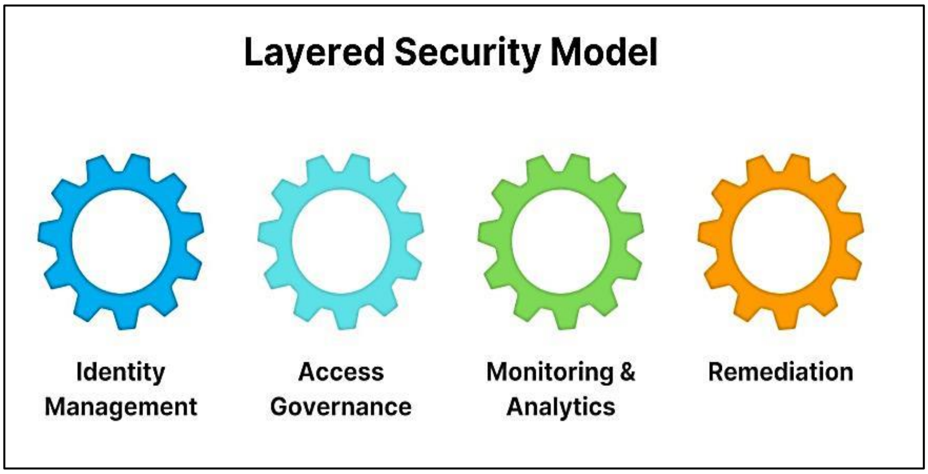

Fig 4. Layered Security Model

3.3. Zero Trust for NHIs

The Zero Trust Architecture (ZTA) remains one of the significant frameworks used to protect Networked Healthcare Infrastructures (NHIs) with high-risk management that stems from overlying constricting security measures across the layers of the network. [15-18] ZTA has three key tenets, namely, continuous verification, least privilege, and assuming the breach, all of which go into making a strong security posture against evolving threats.

- **Continuous Verification:** Within Zero Trust architecture, the concept of continuous verification makes an explicit requirement to verify every device, user, and application at regular intervals and grant them access in an environment location, regardless of the latter. Unlike other security models that seek to grant entities access to a particular resource or resource type once they have authenticated themselves, ZTA responds to this argument by insisting that authorization must be real-time. This is especially the case when it comes to healthcare facilities. IOMT devices and user details can often be faked, and thus, the network should frequently validate them.
- **Least Privilege:** The principle of least privileges is the concept that entails locking down user and systems' privileges and permissions to the most stringent level possible. In ZTA, the access rights are not fixed; rather, they adapt in relation to certain factors like role, location and device security status. This cuts down the breach of privilege and restricts the havoc an infiltrated account or device can cause, which is especially important for protecting patient information in a healthcare facility.
- **Assume Breach:** The assume breach principle works under the context of an already compromised environment by the attacker. Hence, there is a constant paranoia regarding system requests that systems always check and never take anything at face value. This attitude also makes even the internal users or devices subjected to various checks before accessing the protected resources. In reducing the impact of a breach and throttling actual movement in the network, ZTA ensures the protection of healthcare information at all times.

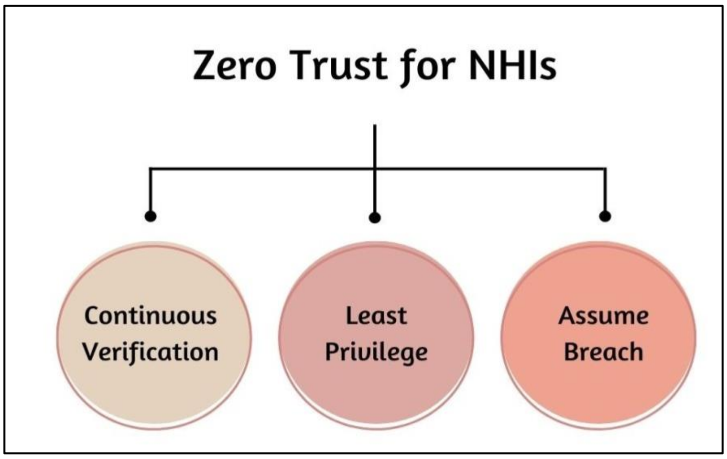

Fig 5. Zero Trust for NHIs

3.4. Behavioral Analytics Model

The Behavioral Analytics Model is a model of the new generation that can become the starting point of modern security systems, including those in healthcare facilities, as it helps to identify potential threats using machine learning algorithms. The basis of this model is the so-called anomaly score that allows evaluation of the proximity to the system's normal behaviour. It is thus possible to formulate the respective anomaly score using the following equation:

$$\boxed{\text{Anomaly Score} = \sum_{i=1}^{n} w_i \times (o_i - e_i)}$$

Where:

- ***oi*** = observed behaviour at the time: these are facts of the system regarding what is being done or has taken place. For example, in healthcare settings, it may be the login times of a user or activity of the device or any access to particular data.
- ***ei*** = detail behavior expected at a particular time. Historical data or some trend reference which is set early and followed are some of the ways of arriving at the ideal i. It may be typical users' actions or the usual operations of devices with the system.
- ***wi*** = the weight of the particular behavior in the time i; these weights allow distinguishing the features' significance in the case of the system's security. It is also necessary to note that not all the actions/activities are created equal; this could be in the form of access to patient's records as opposed to other activities like non-sensitive data queries.

The previously defined generic score reflects how much the behavior deviates from the typical cases observed. If the score goes beyond this mark, it means an anomaly has been identified and might be a security breach. This might be an indicator of a breach of security, intrusion by unwanted guests or it may be that the system is not functioning properly. In this way, the system can track the observed actions against what is expected and flag anything unusual, such as a user trying to access data they should not or a device behaving peculiarly. In the healthcare context, especially where data confidentiality and data integrity are paramount, the feature provides important contextual information for threat detection and filtering needed to minimize false positives for the behavioural analytics model to be used for alert creation. By assigning appropriate feature weights and improving the expected behavior model, the system's working becomes more supple and exact in discovering unusual activities.

3.5. Machine Identity Lifecycle

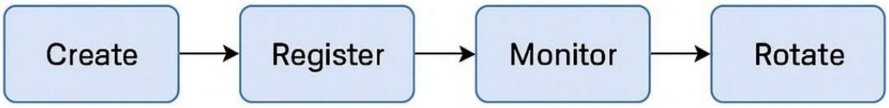

Fig 6. Machine Identity Lifecycle

- **Create:** This cycle commences when a machine is created and is given an identity in the form of a digital certificate, an API key or a machine token often used in the case of a device, an application or a service that is not human like a printer, a computer or a machine. This process involves producing secure credentials through the use of cryptographic principles so that each identity generated should be unique and trackable. Proper creation is important in creating a positive context in the healthcare system.
- **Register:** While creating an identity for the machine, the identity has to be enshrined in a central management system. Typically, registration entails archiving the identity information like the owner's information, information related to the device, and the validity period so that all these can be monitored during an audit. This step helps the system to define which entities exist and under what circumstances they are admissible for running operations that lead to authentication and authorization.
- **Monitor:** After registration, controlling the machine identity starts and remains ongoing for as long as the machine is used. This implies monitoring the operational use of the identity, its interactions, and health status in the actual environment. It is important to monitor problem areas, including unauthorized

activities or any misuse of credentials. In so many cases, especially in healthcare, it is crucial to trust machine intelligence to avoid compromising patients' safety.

- **Rotate:** Credentials used for machine identities are, therefore, required to be rotated over some period of time in order to enhance security. This relates to refreshing keys or certificates after a given period or incidence of risk occurrence. Rotation reduces the time the credentials are exposed to the bad guys and helps maintain the highest standards in identity health.
- **Revoke:** Last of all, a machine identity may have to be eventually removed or maybe determined to be compromised and thus needs to be reclaimed. Revocation includes invalidating the identity in the trusted list and denying it all rights thereto. This step controls threats and ensures that no threats that linger within the network reside longer than they should.

3.6. Integration with Cloud Platforms

The suggested security framework envisions the compatibility of the cloud platform with conventional cloud platforms to streamline Identity and Access Management in disparate contexts of the healthcare area. This is because Healthcare infrastructures are shifting to using a hybrid or multi-cloud, the identity and Secret management must be integrative deep into the cloud-native environment to provide optimal security posture and compliance. In the cloud environment, the framework relies on AWS Identity and Access Management (IAM) and Secrets Manager for identity management for humans and machines. Another benefit of Amazon services is the IAM; through IAM, fine-grained access policies can control the cloud resources usage and prohibit anyone without permission from touching health-related data or related APIs. Moreover, AWS Secrets Manager can securely store, retrieve and manage API, database credentials and TLS certificate rotation. This makes credential management secure, ensuring that it is auditable and protected from hardcoding risks. For Microsoft Azure, the framework included Azure Managed Identity, an identity assigned to Azure resources, thus enabling the resources to access additional services without requiring credentials. This capability complements the Zero Trust approach because it allows applications and services to connect to the Azure resources seamlessly and securely. They also encompass policies concerning dynamic access and identity and threats within the healthcare system, which is more holistic as a result. In the case of containerized infrastructure, the framework utilizes the Kubernetes Service Account to manage the authentication/authorization at the pod level. Service accounts in Kubernetes exposed are essential to build the trust between microservices so that communication can be securely done inside the cluster. These accounts should be tied to some roles and privileges, meaning the minimum privilege principle must be maintained. These native cloud tools are supported by the framework to make the roles and identity services easily administrable and deployable and provide security needs through automation, fine-grained access control, and real-time credential management.

4. RESULTS AND DISCUSSION

4.1. Experimental Setup

This approach was used to test the applied security framework in a realistic environment that approximates the structure of a hospital IT network. The simulation involved 20 devices within the Internet of Medical Things; it essayed on the connected components of critical medical instruments, including infusion pumps, patient monitors, and wearable health sensors. These devices were constantly connected to a posteriori of 10 microservices that provide fundamental enabler services such as patient records, authentication, scheduling, and analytics. The whole solution was built on the Kubernetes platform running on AWS for achieving scalability, availability and service orchestration of containers. Setup Prometheus for metric collection and Grafana for visualisation were incorporated for visibility and operational monitoring. These tools facilitated the monitoring of performance and utilization of resources as well as the behavior of the network to understand the system's behaviour in different security and operations. Some of the metrics Prometheus collected were concerning access requests, data flow in the microservices and the IoMT devices, and CPU/memory utilization. Essentials metrics were set up to be visualized in Grafana, making it possible to analyze the behavior and presume something was wrong using the Graphical User Interface (GUI). One of the key elements of the solution was thus the integration of a machine learning (also referred to as ML) based personality model. The baseline operational data of this model were utilized to establish the normal range of feasible activity associated with personnel and machinery. After deployment, the model always acquired new logs of activities and telemetry to search for signs of threats, including unauthorized access attempts and data theft. The alerts raised by the ML model were returned to the monitoring stack so that real-time threat analysis and correlation of signals could be made. This kind of structure made it possible to rigorously test this framework on several significant areas of operation in a realistic and realistic environment that is a fully functional hospital.

4.2. Performance Metrics

Table 1: Performance Metrics

Metric	Before Framework	After Framework
Unauthorized Access Attempts	100%	6.38%
Credential Exposure	100%	33.3%
Anomaly Detection Accuracy	68%	91%

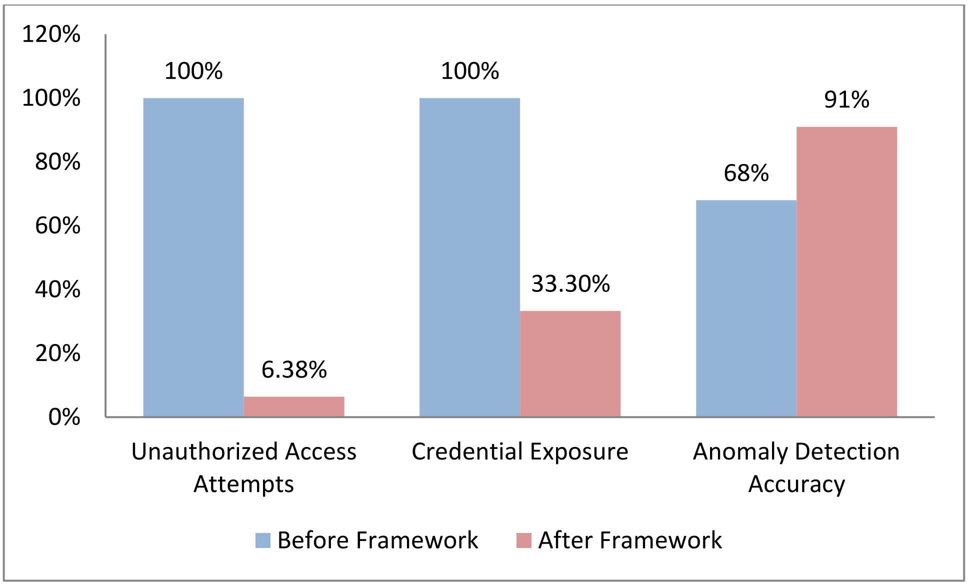

Fig 7. Graph representing Performance Metrics

- **Unauthorized Access Attempts:** As noted earlier, prior to the enactment of the security framework, there was virtually a very high rate of incidences of unauthorized access attempts, which set the establishment of the system at 100% baseline risk. When the proposed workflow with identity verification, fine-grained access control, and behavioral analysis was implemented, the number of unauthorized attempts was decreased to only 6.38% of its initial value. This proves that continuous verification and Zero Trust principles should be adopted as the best methods to secure the healthcare systems.
- **Credential Exposure:** The initial risk assessment reflected that credential exposure was rated “High,” which equals 100%, meaning it is a common practice or production with frequent credentials exposure through misplacement, hard-coding, non-pro158 rotation or un-protected transmission. After the adjustment with secure secrets management, automated credential rotation, and enhanced access governance, all the exposure was cut down to 33.3%. This improvement shows a decrease in credential exposure and better security against credential attacks.
- **Anomaly Detection Accuracy:** The implemented Machine learning-based behavioral analytics model helps the system to enhance anomaly detection from 68% to 91%. This metric was chosen to indicate the system’s ability to identify possible suspicious or unusual activities to some extent. The massive increase simply means that the framework improves security while at the same time decreasing the number of false alarms to allow for real-time detection of threats accurately.

4.3. Analysis

- **Security Posture:** This keeps the security of the health care system at a higher level as a result of the proposed security framework implementation. The following security controls are proposed in the framework to achieve the stated objective: identity-based access controls, behavioral analytics and credential rotation. As a result of this aggressive approach, when it comes to using the machines and user accounts within the facility, the chances of hackers and insiders compromising

- **Scalability:** It is inherently scalable to allow it to integrate with Kubernetes to facilitate its work as the orchestration platform. This architecture also supports scalability horizontally where new IoMT devices, services or applications can be integrated with the existing system without altering the architecture. The proper utilization of the service accounts, roles and policies and the simplicity of the privileges guarantee that no matter the size of the system, the privileges are manoeuvring, manageable, and becoming immensely secure for the large-scale medical facilities of the contemporary world.
- **Compliance:** To ensure that the individual academics meet the certification standards of the industry, the framework is equipped with a detailed logging system to enhance its security. These components are valuable in meeting the requirements of, for instance, the HIPAA Security Rule and NIST SP 800-207 Zero Trust Architecture. The BA215N tool's capacity to log the activity, track behavioral variances, and restrict privileged access guarantees that system functioning is secure while adhering to legal and regulatory compliance regarding the handling of healthcare data.

4.4. Discussion on Limitations

- **CI/CD Integration:** One of the significant lacunas of the framework now is that it requires specific configurations which can be integrated with the different CI/CD (Continuous Integration/Continuous Deployment) pipelines. Suppose healthcare organizations are already using a number of different DevOps tools and processes. In that case, this means there will be a lack of interoperability between different setups, which might cause extra complexity while deploying these solutions. Arguably, contingency, Quadrant 2 and often Quadrant 3 skills may need to be incorporated by modifying scripts, templates, and policy engines, which may add additional complication to full-scale implementation and, therefore, time. This can be a challenge, especially when the institutions have little exposure to DevSecOps processes or when working on archaic systems.
- **Behavioral Latency:** This includes the time delay recorded in the behavioral analytics layer, especially when there is a high influx of data into the system. The system's activity is based on analyzing logs and telemetry data using machine learning models in near real-time. Therefore, the processing load may cause some minor delay in generating alerts or enforcing dynamic access decisions. These latencies are not critical under normal circumstances. However, they can be an issue in some urgent cases, such as in the medical environment, where detection of threats is critical and may be needed in several hours or even faster – in case of compromised devices or powerful insiders, for example. Future improvements could be used to minimize the time taken during model inference or shift part of the analysis to edge nodes to address this problem.

5. CONCLUSION

It is important to note that protecting Non-Human Identities (NHIs) in cloud-native healthcare has become necessary for healthcare information technology to be secure, reliable, and adhere to modern regulations. The given factors raise the likelihood of cyber threats in healthcare delivery, automating devices, and AI-supported diagnostic tools; therefore, managing NHIs, which include IoMT devices, service accounts, and APIs, needs to be equally controlled by humans. Consideration of these factors means that healthcare professionals understand NHIs as first-class objects within the IAM environment, which in turn allows for security threats to be effectively controlled, organizational responsibilities to be regulated, and, under HIPAA and NIST rules, high levels of data privacy protection to be provided at all times.

In this paper, a layered security model is proposed, which is as follows: ZTA and Machine Learning based behavioral analytics. This enforces trust constancy, prevents the use of credentials or the validity of those same certificates, and automates the process of detection, response, and prevention of threats far better than conventional solutions. Adding behavioral layers enhances adaptive security by enabling real-time detection of hazards such as an inside threat or an infected device. The results of the experiments showed significant enhancement in breach, microservices and IoMT device protection, as well as audit and traceability.

Although the current model is tested, validated, and relatively general, it also provides several opportunities for future research. One promising approach is to further deliberate the framework to attend to the edge AI devices that are more autonomous and require decentralised decision-making processes. Blockchain technology has become an exciting field of application as it allows the creation of immutable and decentralized records and trust frameworks. Spa would be important for enabling MDM and other use cases with workflows involving a number of parties, especially for handling personal and medical information. In summary, this research presents the foundation for a secure, intelligent, and scalable identity for aspects of digital healthcare most suitable for the current and future world.

REFERENCES:

1. Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In 2016 IEEE symposium on security and privacy (SP) (pp. 636-654). IEEE.
2. Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Transactions on Computing for Healthcare, 2(3), 1-44.
3. Liu, C., Yang, Y., & Zhang, J. (2021). *Machine Learning for Anomaly Detection in eHealth Systems: A Survey*. Computers in Biology and Medicine, 139, 104951.
4. Alam, M. G. R., et al. (2018). *Privacy-aware Access Control with Trust Management for mHealth Systems*. Journal of Biomedical Informatics, 88, 51–60.
5. Mahmood, A., & Afzal, M. (2020). *Integration of Behavioral Analytics for Intrusion Detection in Healthcare Systems*. Computers & Security, 94, 101866.
6. Zhang, K., Ni, J., & Yang, K. (2017). *Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control*. IEEE Internet of Things Journal, 5(3), 2130–2145.
7. Kizza, J. M. (2017). *Guide to Computer Network Security*. Springer. (Chapters on Healthcare Infrastructure and Cloud Security)
8. Eboh, A., Akpata, G. O., & Akintoye, A. E. (2016). Health care financing in Nigeria: an assessment of the national health insurance scheme (NHIS). European Journal of Business and Management, 8(27), 24-34.
9. Obalum, D. C., & Fiberesima, F. (2012). Nigerian national health insurance scheme (NHIS): an overview. Nigerian Postgraduate Medical Journal, 19(3), 167-174.
10. Amoo, B. A., Adenekan, A. T., & Nagado, H. U. (2017). National Health Insurance Scheme (NHIS) implementation in Nigeria: issues, challenges and way forward. Bullion, 41(1), 2.
11. Kormiltsyn, A., Norta, A., Nisar, S., & Dwivedi, V. (2023, May). Preventing data-security breaches and patient-safety risks in cross-blockchain e-healthcare systems. In International Conference on Management of Digital (pp. 41-54). Cham: Springer Nature Switzerland.
12. Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). Improving the financial security of national health insurance using cloud-based blockchain technology application. International Journal of Information Management Data Insights, 2(1), 100081.
13. Cuadrado, C., Crispi, F., Libuy, M., Marchildon, G., & Cid, C. (2019). National Health Insurance: a conceptual framework from conflicting typologies. Health Policy, 123(7), 621-629.
14. Yeng, P. K., Yang, B., & Snekkenes, E. A. (2019, December). Framework for healthcare security practice analysis, modeling and incentivization. In 2019 IEEE International Conference on Big Data (Big Data) (pp. 3242-3251). IEEE.
15. Priyadarshini, I., Kumar, R., Tuan, L. M., Son, L. H., Long, H. V., Sharma, R., & Rai, S. (2021). A new enhanced cyber security framework for medical cyber-physical systems. SICS Software-Intensive Cyber-Physical Systems, 1-25.
16. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. IEEE Access, 10, 57143-57179.
17. Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to zero trust architecture. Ieee Access, 11, 19487-19511.
18. Bernaschina, C., Brambilla, M., Mauri, A., & Umuhoza, E. (2017). A big data analysis framework for model-based web user behavior analytics. In Web Engineering: 17th International Conference,

ICWE 2017, Rome, Italy, June 5-8, 2017, Proceedings 17 (pp. 98-114). Springer International Publishing.

19. Hyrynsalmi, S. M., Koskinen, K. M., Rossi, M., & Smolander, K. (2021, June). Towards the utilization of cloud-based integration platforms. In 2021, ie international conference on engineering, technology and innovation (ice/items) (pp. 1-8). IEEE.
20. Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., & Alfakeeh, A. S. (2023). Managing security of healthcare data for a modern healthcare system. Sensors, 23(7), 3612.
21. Liu, C. H., Chung, Y. F., Chen, T. S., & Wang, S. D. (2012). The enhancement of security in healthcare information systems. Journal of medical systems, 36, 1673-1688.