Strengthening Zero Trust Security Framework Towards Hospital Management

VAJRATIYA VAJROBOL

[1] International Center for AI and Cyber Security Research and Innovations. Asia University, Taiwan.
(e-mail: vvajratiya@gmail.com).

ABSTRACT Cyberattacks are increasingly focusing on the healthcare sector. This is because hospitals hold sensitive data, including financial and medical details on patients. Hospitals frequently have intricate networks and systems, which makes them challenging to safeguard. A novel approach to cybersecurity called "zero trust security" can help hospitals strengthen their security posture. The idea behind zero trust is "never trust, always verify." This means that regardless of whether they are inside or outside the network perimeter, all users and devices are authenticated before being given access to resources. This research aims to propose and implement a comprehensive zero-trust framework tailored to hospital management. By leveraging technologies such as micro-segmentation, multi-factor authentication, and continuous monitoring, this framework will enhance the security landscape of hospitals, with a primary focus on safeguarding the integrity and confidentiality of patient data.

KEYWORDS zero trust, cybersecurity, hospital management, healthcare.

I. INTRODUCTION

Hospitals have become popular targets for bad actors as the number of cyberattacks targeting the healthcare sector has increased alarmingly. The large quantities of sensitive data, including patient health records, financial data, and research data, that healthcare organizations store make them particularly alluring targets. The complex web of networks and systems that hospitals rely on to provide patient care and oversee crucial operations adds to the difficulty of this problem. It has become critical to secure these complex ecosystems.

In this era of sophisticated and persistent attacks, traditional methods of cybersecurity that were based on the idea of a trusted internal network and a well-defined perimeter are no longer sufficient. Hospitals need to change the way they approach security so that they can take into account the vulnerabilities that are already there. Zero Trust Framework, is a ground-breaking and proactive approach to cybersecurity with enormous potential for the healthcare industry.It is based primarily on the tenet "never trust, always verify." (Vukotich, 2023). According to this paradigm shift, no person or device should ever be given complete trust, regardless of whether they are inside or outside the network perimeter. Instead, before being allowed access to vital resources, all entities must pass strict verification. Microsegmentation, multi-factor authentication, and continuous monitoring are just a few of the powerful technologies that Zero Trust uses to enforce these principles. This study intends to examine the significant advantages a Zero Trust Framework can offer hospital management. Hospitals may drastically improve their security posture and protect patient data by implementing a Zero Trust strategy.

The research is structured as follows: it commences with an introduction, followed by a review of prior studies. Next, it presents the proposed framework for implementing zero trust security in hospital management settings. Subsequently, it delves into future trends concerning zero trust in the healthcare sector, discusses the challenges inherent in adopting this approach, and explores the potential for AI-assisted enhancements within the zero trust framework. Finally, the research concludes by summarising key findings and offering insights into the broader implications of strengthened healthcare cybersecurity.

II. LITERATURE SURVEYS

The term "zero trust" gained popularity in 2010 when analyst John Kindervag of Forrester Research said that an organization should not have any trust whatsoever, either inside or beyond its boundaries. The zero-trust security approach had a major increase in usage in 2021. Microsoft's "Zero Trust Adoption Report" (2021) for that year states that an astounding 96% of the 1,200 security decision-makers polled emphasized how crucial zero trust is to the success of their organizations. The urgent requirement for increased security and compliance agility as well as the desire to hasten the identification and removal of cybersecurity threats were major driving forces behind its adoption. Furthermore, according to the research, the increasing adoption of the zero-trust paradigm was largely driven by the extensive use of remote work arrangements and hybrid work during the COVID-19 epidemic.

Numerous prior research has examined the lack of trust in healthcare. A zero-trust architecture-based security awareness and protection system for 5G-based smart medical systems is presented by Chen et al. (2020). The "subject" (people, terminals, and applications), "object" (data, platforms, and services), "behaviour," and "environment" are the four main dimensions that this system concentrates on. It creates models for dynamic access control, accomplishes situational awareness of network security in real time, authenticates users continuously, examines access patterns, and applies fine-grained access control.

A framework based on zero-trust principles was created by Tyler & Viana (2021) to assist healthcare businesses in implementing more secure systems. The framework was successfully tested in Cisco Modelling Labs (CML), proving that the main goal of minimising harm in the event of a compromised host within the local area network (LAN) was accomplished. Furthermore, it was shown that placing firewalls right in front of medical equipment improves network efficiency by preventing unneeded traffic—despite being unusual and possibly adding latency.

The proposed paradigm by Ali et al. (2021) entirely trusts User Equipment (UE) after verifying the validity of user credentials, which are converted into encrypted data. Through the smooth integration of diverse technologies such as computers, medical equipment, and telecommunications, there exists a significant possibility to improve patient care efficacy, reduce healthcare costs, and strengthen privacy and security protocols.

III. PURPOSED FRAMEWORK

The Zero Trust Framework has gained attention as an essential cybersecurity strategy, particularly in the healthcare industry where patient data privacy and the security of important medical systems are paramount. Adopting a Zero Trust Framework in hospital administration involves a comprehensive plan composed of seven different components. Together, these aspects serve as a fundamental component of security that preserves the confidentiality and integrity of healthcare activities.As seen in Figure 1, the framework consists of seven components: data classification and protection, network segmentation, identity and access management (IAM), continuous monitoring and anomaly detection, security awareness and training, endpoint security and vendor and third-party risk management.

3.1. Data Classification and Protection

The Zero Trust Framework's Data Classification and Protection aspect offers a comprehensive strategy for protecting sensitive data in the context of hospital management. The first step in the process is "Data Discovery and Identification," which calls for healthcare organisations to have a thorough grasp of the location and attributes of their data assets. This calls for the application of sophisticated data finding methods and technologies that can navigate the complex network and system architecture seen in contemporary hospitals. Healthcare organisations lay the groundwork for a shift to data-centric security by identifying data repositories and endpoints.

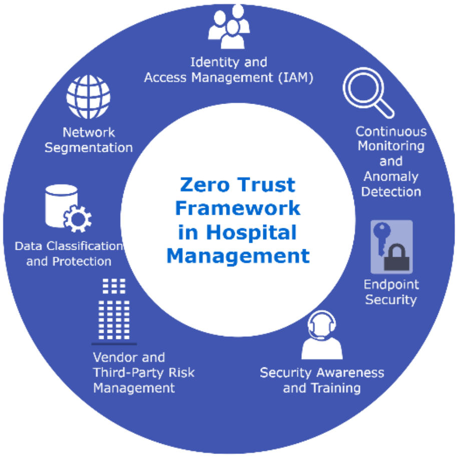
Identity and Access Management (IAM)
Continuous Monitoring and Anomaly Detection
Endpoint Security
Security Awareness and Training
Vendor and Third-Party Risk Management
Data Classification and Protection
Network Segmentation
Zero Trust Framework in Hospital Management

Figure 1. Zero Trust framework in Hospital Management

"Data Categorization and Sensitivity Labelling" is the next step. This is a crucial stage where data is categorised into different classifications according to sensitivity levels. Common classifications like "Sensitive," "Highly Sensitive," and "Non-sensitive" are commonly used. (Shahid et al., 2021).Every category aligns with distinct security specifications, guaranteeing that vital resources like medical records, financial information, and research data are adequately safeguarded. Data sets are given sensitivity labels or tags, which make it easier to apply encryption standards and access controls that are tailored to the value of the data.

Hospital data security is greatly aided by the use of encryption strategies, both in transit and at rest. Two crucial times when encryption is used are when data is in transit and when it is at rest. Data is encrypted when it travels over the hospital network using secure communication protocols like Transport Layer Security (TLS) (Zarate, 2021).Because of the encryption, the data is protected against interception and compromise by being unintelligible to possible eavesdroppers. Encryption techniques like the powerful Advanced Encryption Standard (AES) are used to safeguard data at rest, whether it is kept in file servers, databases, or other storage systems (Renardi et al., 2018). Establishing a strong Key Management system is essential to encryption because it guarantees the safe generation, storage, and regular rotation of encryption keys, strengthening the security posture as a whole (Kuzminykh, 2020).

One further essential component of the Zero Trust system is access control mechanisms. Strict access controls must be put in place to guarantee that data can only be accessed by authorised individuals and only in certain circumstances. While Attribute-Based Access Control (ABAC) takes into account extra attributes like user location and device state when making access choices, Role-Based Access Control (RBAC) grants permissions to users based on their designated responsibilities within the institution (Choksy et al., 2023 ; de Carvalho Junior & Bandiera-Paiva, 2018).Access policies specify which users can access particular data and the conditions under which access is allowed. They are carefully drafted and strictly enforced. Additionally, by constantly monitoring and stopping unwanted data transfers, the implementation of Data Loss Prevention (DLP) Measures actively enforces access rules and successfully confines sensitive data within approved bounds (Alneyadi & Muthukkumarasamy, 2016).

Finally, hospitals understand how important it is to follow secure disposal procedures and data retention policies. Policies are in place to ensure suitable retention periods for data, as it is not recommended to retain data indefinitely. This proactive strategy removes redundant data, hence reducing the attack surface. Secure Data Disposal, which includes actions like disk wiping and data shredding, is equally important. By ensuring that data becomes unrecoverable at the end of its lifecycle, these precautions reduce the possibility of data breaches resulting from incorrect information being deleted.

3.2. Network Segmentation

Network segmentation stands out as a key component of the Zero Trust paradigm in the larger context of hospital administration, significantly altering cybersecurity procedures. The implementation of Micro-Segmentation Strategies embodies the granularity that is fundamental to Network Segmentation. For this reason, hospitals with complex infrastructures choose to create highly specialised security zones instead of depending on a single network perimeter. These zones are the result of micro-segmentation and are carefully planned to serve certain functions or user groups. This fine-grained segmentation hinders potential attackers' lateral movement and makes it more difficult for them to traverse the network after a compromise (Sheikh et al., 2021).

Furthermore, the Clinical and Administrative Network Separation is required by the special requirements of healthcare facilities. This method acknowledges the vital necessity of separating administrative systems like HR and finance from clinical networks, which house electronic health records and patient care systems. In addition to protecting patient information, this division acts as a barrier against attacks that could compromise vital healthcare infrastructure (Syed et al., 2022)

The Zero Trust Framework promotes the isolation of medical devices in a time when they are essential to healthcare. These gadgets, which include patient monitors and infusion pumps, frequently have flaws that could be used by hostile actors. Devoted segments are created to lessen these dangers; in the event that a medical device is compromised, the attackers' ability to move laterally is restricted, lowering the exposure of the wider network.

The idea of a Perimeter-Less Network Design, which is a radical divergence from conventional security approaches, is central to the Zero Trust paradigm. It recognizes that modern threats are dynamic and can come from both inside and beyond the network perimeter. Rather than depending exclusively on conventional firewalls, Zero Trust views every network segment as a possible boundary for security. By defining and constantly monitoring access policies, a monolithic firewall is not necessary (Yan & Wang, 2020)

The Zero Trust Networking Principles regulate the fundamentals of Network Segmentation inside the Zero Trust Framework. The foundation of trust presumptions in the network architecture is formed by these ideas. They stipulate that no user, device, or system—regardless of location—must undergo thorough verification before being able to access network resources, and that confidence should never be taken for granted. This strict methodology includes careful access control enforcement, strict authentication procedures, and ongoing monitoring.Segmentation enforcement mechanisms must be implemented in order to operationalize network segmentation. These cover a wide range of technologies, such as network access control (NAC) systems, software-defined networking (SDN) solutions, and next-generation firewalls (Baird et al., 2017).

Healthcare organisations can now establish, monitor, and enforce security zones and keep an eye out for unusual network traffic patterns thanks to these tools. Within the Zero Trust Framework, network segmentation becomes an essential tool for healthcare organisations facing an ever-increasing barrage of cyber threats. In terms of hospital administration, it strengthens patient data security, protects vital healthcare infrastructure, and adheres to the Zero Trust paradigm.

3.3 Identity and Access Management (IAM)

Identity and Access Management (IAM) has a central position in the overall hospital management environment as a crucial element of the Zero Trust Framework. IAM is a comprehensive approach to carefully managing and safeguarding user identities and their access to vital medical resources.

Using Strong Authentication Methods is a cornerstone of IAM inside the Zero Trust Framework (Yan & Wang, 2020). Hospitals have strong authentication procedures that go beyond standard username and password combinations because they recognize the increased cybersecurity risks they confront. Among the techniques used are smart card-based authentication, biometric authentication, and multi-factor authentication (MFA) (Suleski et al., 2023). By requiring users to undergo stringent verification before accessing healthcare systems and data, these techniques lower the possibility of unwanted access.Another tenet of IAM is the

Least Privilege Access Model concept. Hospitals support the idea that users should only be allowed the minimal amount of access necessary to carry out their particular responsibilities. This strategy reduces the attack surface and limits the possible harm that could be caused in the case of a breach (Plachkinova & Knapp, 2022).

IAM solutions heavily rely on the techniques of Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC). Users are granted permissions through RBAC according to their assigned positions in the hospital. By taking into account extra factors like user location and device status when determining access, ABAC, on the other hand, expands access control. These adaptable access control models guarantee that each user's access to critical healthcare systems and data is specifically catered to their needs (Sanders & Yue, 2019)

IAM frameworks, which include Access Policy Definition and Enforcement, carefully create and implement access policies. These guidelines specify who has what amount of privilege, when they can access particular resources, and under what circumstances. Hospitals maintain strict adherence to set policies by means of ongoing monitoring and enforcement.

IAM in healthcare requires User Lifecycle Management. This includes the entire user experience—from onboarding to offboarding—within the healthcare environment. The procedure entails provisioning users, adjusting access privileges in response to changing roles, and securely deprovisioning users' access upon terminating their affiliation with the institution. Effective management of the user lifecycle reduces the possibility of residual access privileges and improves security in general.

3.4. Continuous Monitoring and Anomaly Detection

An essential part of the Zero Trust Framework for hospital administration is Continuous Monitoring and Anomaly Detection. Real-time threat detection and response capabilities are critical in high-stakes environments.At the heart of this effort are real-time monitoring solutions. Modern technologies are used by hospitals to keep an eye on user behaviour, system activity, and network traffic. Security professionals can quickly spot possible security breaches or unusual activity thanks to this real-time visibility (Singh et al., 2023)

The hospital's security posture is further strengthened through the use of Behavioral Analytics for Threat Detection. Hospitals can efficiently identify aberrations that can signal to malicious activity by setting baselines of typical user and system behaviour. Algorithms for behavioural analytics examine trends and abnormalities to identify possible dangers before they become serious. The concept of Machine Learning-Driven Anomaly Detection is extended further. The intricacies and subtleties of anomalies that conventional rule-based detection methods could miss are easily detected by machine learning techniques. These cutting-edge algorithms improve the hospital's capacity to recognize new dangers by continuously learning from data trends and modifying their threat detection skills (Javaid et al., 2022).

The Zero Trust Framework is reliant on automated processes for threat detection and response. Hospitals use automated systems that have the ability to both identify abnormalities and launch pre-programmed responses. This ability to act quickly is essential for reducing risks before they have a chance to cause significant harm.A essential procedure for anomaly identification and continuous monitoring is event and incident logging. Hospitals keep thorough records of all events and incidents pertaining to security. Security teams may recreate events, examine security breaches, and improve security procedures with the use of these logs, which are essential forensic tools.The foundation of anomaly detection and continuous monitoring is the integration of Security Information and Event Management (SIEM). Hospitals incorporate SIEM systems, which collect, correlate, and evaluate network-wide security-related data. SIEM systems facilitate real-time threat detection, incident response, and reporting by offering a centralised view of security events (Kavanagh et al., 2015)

3.5. Endpoint Security

One essential component of the Zero Trust Framework designed specifically for hospital administration is endpoint security. Workstations, medical equipment, mobile devices, and other endpoints make up the intricate web of hospital networks, and all of them can be points of entry for cyberattackers. It is crucial to make sure these endpoints are secure.

Secure Device Configuration Standards are the cornerstone of endpoint security that works. Hospitals implement strict configuration guidelines that require all network-connected devices to have secure settings. This covers both common workstations and specific medical equipment. Following these guidelines makes devices less vulnerable to exploitation and helps to minimise vulnerabilities (Wani et al., 2020)

Protecting endpoints is mostly dependent on endpoint protection solutions like antivirus software and endpoint detection and response (EDR) systems. Strong antivirus programs are used by hospitals to constantly check equipment for malware and other harmful applications. On the other side, improved threat detection and response capabilities offered by EDR solutions enable security teams to quickly identify and neutralise attacks (Martin & Bruno, 2022).

Patch management and vulnerability assessment are essential procedures for preserving endpoint security. Hospitals frequently check their equipment for security flaws and quickly install updates and patches. By patching vulnerabilities before attackers can exploit them, this proactive method lowers the attack surface.

Application blacklisting and whitelisting are essential parts of endpoint protection. Whitelisting is a tool used by hospitals to restrict which applications are permitted to operate on endpoints, making sure that only programs that are trusted and authorised can function. On the other hand, blacklisting strengthens endpoint security by preventing the execution of known malicious or unapproved programs (Chandel et al ., 2019)

Robust Mobile Device Management (MDM) solutions are required due to the growth of mobile devices in the healthcare industry. Hospitals use mobile device management (MDM) solutions to control and safeguard mobile devices, enforce security guidelines, and make sure these devices don't endanger the network. In the event that a device is lost or stolen, this includes the capability to remotely wipe or lock it (Sisala & Othman, 2020).

Active response capabilities are included in the implementation of Endpoint Detection and Response (EDR), which goes beyond threat detection. In order to control and eliminate threats, hospitals use EDR solutions that not only recognize suspicious behaviour but also allow automated reactions or start manual activities. In order to keep a secure endpoint environment, a hospital needs to have this real-time reaction capabilities.

3.6. Security Awareness and Training

The Zero Trust Framework, which is specifically designed for hospital administration, highlights Security Awareness and Training as essential foundational elements. Strong technical protections are necessary, but people are still a critical component in guaranteeing healthcare organisations' overall security posture.The foundation of a successful security awareness campaign is comprehensive security training programs. Hospitals use formal training programs to teach staff members of all ranks about different facets of cybersecurity. These courses cover anything from identifying phishing attempts to comprehending best practices for security.

Exercises that teach phishing awareness and simulation are essential components of hospital security training. Hospitals use phishing campaign simulations to teach staff members about the strategies used by online fraudsters. By teaching users to identify phishing efforts, malicious emails, and fraudulent correspondence, these exercises ultimately lower the likelihood that users will become victims of these types of assaults. (Katsikas , 2000 ; Alhuwali et al., 2021).

In healthcare facilities, user education on security best practices is a continuous project. Hospitals ensure that staff members are knowledgeable on security best practices, which include safe surfing practices, password management, and secure data processing. Ongoing instruction strengthens a security-conscious society.A constantly changing threat landscape necessitates ongoing training and updates. Hospitals view security training as a continuous activity rather than a one-time occurrence. Employees are kept up to date on the newest security precautions and threats through regular updates and refresher sessions.

A comprehensive strategy called "security culture building" seeks to inculcate a security-aware mindset across the entire company. A culture where everyone is accountable for security is fostered by hospitals. Employees now actively contribute to the protection of patient data and healthcare systems as a result of this cultural shift.It is essential to provide reporting and incident response training to staff members so they are prepared to handle security incidents or breaches. In order to facilitate prompt reaction and containment of security risks, hospitals offer training on incident reporting processes.

3.7. Vendor and Third-Party Risk Management

One of the most important components of hospital administration's Zero Trust Framework is vendor and third-party risk management. Regular interactions between healthcare facilities and outside vendors and third-party service providers may expose them to risks. Hospitals set strict procedures for handling these outside contacts in order to protect patient information and uphold security.

The cornerstone of third-party and vendor risk management is a Third-Party Assessment Framework. Hospitals establish precise standards for evaluating outside organisations' security procedures. This framework guarantees that third parties follow the institution's security criteria and directs the review process (Kandasamy et al. 2020).

Hospitals set Strong Security Requirements for Vendor in order to reduce the risks connected with external collaborations. These stipulations stipulate that vendors must fulfill particular security norms and procedures in order to conduct business with the hospital. By taking this proactive stance, the hospital can make sure that outside parties respect its security posture.Verifying the security procedures of external partners is made possible through the use of vendor security audits and compliance checks. In-depth security audits and compliance checks are carried out by hospitals to make sure that vendors follow the specified security protocols. These audits are a way to find security holes and fix them.

To control the sharing of private medical information with other parties, secure data sharing protocols have been developed. To safeguard data while it's in transit, hospitals use encryption techniques and secure protocols. These protocols guarantee the confidentiality and integrity of patient data while it is being transmitted. In the event of a third-party security incident, preparation is crucial. Hospitals mandate the implementation of Third-Party Security Incident Response Plans for their external partners. In the case of a breach, these plans specify how outside parties will react to security events and work in tandem with the hospital's incident response teams. Maintaining compliance and security alignment requires constant monitoring of vendor security practices. Hospitals see vendor security as a continuous effort rather than a one-time evaluation. Healthcare organizations can confirm that vendors continuously adhere to security standards by conducting ongoing monitoring.

IV. NEXT DEVELOPMENTS AND ASPECTS TO TAKE INTO ACCOUNT FOR HEALTHCARE ZERO TRUST SECURITY

Threat actors' continual ingenuity and the quick development of technology mean that the cybersecurity landscape is always changing. The healthcare sector's adoption of the Zero Trust security architecture is expected to undergo a substantial evolution in this ever-changing environment. This section explores upcoming trends and factors, such as developing technologies, obstacles, changing threat vectors, and the critical role of AI and machine learning, that will influence the application of Zero Trust in healthcare.

4.1.Zero Trust Micro-Segmentation: The development and application of micro-segmentation methods is one of the newer aspects of Zero Trust in the healthcare industry. Hospitals are using micro-segmentation more frequently in order to establish more precise security zones and restrict the ability of possible attackers to move laterally. This technique lowers the attack surface, improves visibility, and gives network traffic more accurate control (Basta et al., 2022).

4.2. Zero Trust Access for IoT and Medical Devices: As Internet of Things (IoT) devices proliferate and become more integrated into healthcare settings, there is an increasing need to apply the principles of Zero Trust to these devices as well. In order to ensure that they do not jeopardise overall network security, emerging technologies will concentrate on safely integrating and managing IoT and medical devices inside the Zero Trust framework (He et al., 2022).

4.3 Continuous Authentication: In a dynamic healthcare setting, traditional authentication methods—even those that use multi-factor authentication (MFA)—may not be as effective. Emerging technologies will investigate continuous authentication techniques to make sure that user confidence is continuously verified during their sessions, like behavior-based authentication and biometric verification (Al-Naji & Zagrouba, 2020).

V.POSSIBLE DIFFICULTIES AND CHANGING THREAT VECTORS

5.1. Insider Threats: Whether deliberate or unintentional, insider threats will continue to be a major worry for healthcare organizations as they digitize their operations. As Zero Trust advances, increasingly more complex systems for identifying and addressing insider threats—including those involving medical professionals—will be required (Ayala & Ayala, 2016).

5.2. Ransomware and Extortion: The methods used by cybercriminals are changing, and ransomware attacks are becoming more common. Subsequent versions of Zero Trust should concentrate on preventing ransomware attacks, and they should consider including real-time backup and recovery techniques to reduce downtime in the case of an attack (Minnaar & Herbig, 2021).

5.3 Cloud Security: There are advantages and disadvantages to moving healthcare services and data to the cloud. Future Zero Trust systems must smoothly interact with cloud security measures as healthcare organizations continue their journey toward cloud adoption, guaranteeing that data is protected wherever it is (Casola et al., 2016).

VI. MACHINE LEARNING AND AI's PLACE IN ZERO TRUST SECURITY

Machine learning (ML) and artificial intelligence (AI) are going to be essential to the development of zero trust in healthcare.

6.1 Threat Detection and Prediction: Pattern recognition and anomaly detection are areas where AI and ML systems shine. These tools will be crucial for seeing new dangers and anticipating any security lapses before they happen. Large-scale datasets can be analysed by machine learning models to find departures from baseline behaviours, which can then be used to trigger alerts for quick action (Hamid et al., 2016).

6.2 Behavioral Analytics: AI-powered behavioural analytics programs will track device and user activity all the time in the healthcare setting. AI is able to identify anomalies that point to security breaches, whether they are the result of insider threats or foreign attackers, by setting baselines for typical behaviour (Saeli et al, 2020).

6.3. Adaptive Access Control: By dynamically modifying user privileges in response to real-time risk assessments, artificial intelligence can improve access control methods. Access may be blocked or extra authentication procedures may be required if AI notices odd behaviour or a possible threat (Song et al ., 2017).

VII. CONCLUSIONS

In conclusion, the complexity of hospital networks and the sensitivity of stored data make the healthcare sector vulnerable to cyberattacks, which emphasises the urgent need for strong cybersecurity defences. Hospital security posture can be improved with the help of the Zero Trust Framework.

The tenet of Zero Trust—"never trust, always verify"—resonates particularly in the healthcare industry, where data breaches can have grave repercussions. Microsegmentation, multi-factor authentication, and continuous monitoring are examples of technology that hospitals can use to implement Zero Trust, which provides a proactive protection against cyber attacks.

This study has put out a thorough Zero Trust Framework specifically designed for hospital administration, highlighting seven significant elements to safeguard patient information and vital healthcare systems. Data classification and protection, network segmentation, identity and access management, endpoint security, security awareness and training, continuous monitoring and anomaly detection, and vendor and third-party risk management have all been discussed in detail.

Furthermore, the study has clarified upcoming developments and factors to be taken into account in Zero Trust security for healthcare, such as developing threat vectors, new technologies, and the revolutionary potential of AI and machine learning.

Adopting the Zero Trust Framework is not only a wise decision, but also a requirement in the quickly changing digital ecosystem where the healthcare sector must contend with ever-more-sophisticated cyber attacks. Hospitals may strengthen their defences, protect patient data, and guarantee the integrity of vital medical systems by implementing Zero Trust principles and remaining alert to new threats. Integrating Zero Trust security principles will be essential to maintaining the healthcare industry's resilience in the face of changing cybersecurity concerns as it continues to embrace technology.

References

Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & AlDuaij, S. (2021). Information security awareness and behaviors of health care professionals at public health care facilities. *Applied Clinical Informatics*, *12*(04), 924-932.

Ali, B., Gregory, M. A., & Li, S. (2021, November). Uplifting healthcare cyber resilience with a multi-access edge computing zero-trust security model. In *2021 31st international telecommunication networks and applications conference (itnac)* (pp. 192-197). IEEE.

Al-Naji, F. H., & Zagrouba, R. (2020). A survey on continuous authentication methods in Internet of Things environment. *Computer Communications*, *163*, 109-133.

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage prevention systems. Journal of Network and Computer Applications, 62, 137-152.

Ayala, L., & Ayala, L. (2016). Hospital insider threat. *Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention*, 47-51.

Basta, N., Ikram, M., Kaafar, M. A., & Walker, A. (2022, April). Towards a zero-trust micro-segmentation network security strategy: an evaluation framework. In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium* (pp. 1-7). IEEE.
Casola, V., Castiglione, A., Choo, K. K. R., & Esposito, C. (2016). Healthcare-related data in the cloud: Challenges and opportunities. *IEEE cloud computing*, *3*(6), 10-14.

Baird, M., Ng, B., & Seah, W. (2017). WiFi network access control for IoT connectivity with software defined networking. In *Proceedings of the 8th ACM on Multimedia Systems Conference* (pp. 343-348).

Chandel, S., Yu, S., Yitian, T., Zhili, Z., & Yusheng, H. (2019, October). Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat. In *2019 international conference on cyber-enabled distributed computing and knowledge discovery (cyberc)* (pp. 81-89). IEEE.

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., ... & Zhai, Y. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, *8*(13), 10248-10263.

Choksy, P., Chaurasia, A., Rao, U. P., & Kumar, S. (2023). Attribute based access control (ABAC) scheme with a fully flexible delegation mechanism for IoT healthcare. *Peer-to-Peer Networking and Applications*, 1-23.

de Carvalho Junior, M. A., & Bandiera-Paiva, P. (2018). Health information system role-based access control current security trends and challenges. *Journal of healthcare engineering*, *2018*.

Hamid, Y., Sugumaran, M., & Journaux, L. (2016, August). Machine learning techniques for intrusion detection: a comparative analysis. In *Proceedings of the International Conference on Informatics and Analytics* (pp. 1-6).

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

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Rab, S. (2022). Significance of machine learning in healthcare: Features, pillars and applications. *International Journal of Intelligent Networks*, *3*, 58-73.

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(1), 1-18.

Katsikas, S. K. (2000). Health care management and information systems security: awareness, training or education?. *International journal of medical informatics*, *60*(2), 129-135.

Kavanagh, K. M., Rochford, O., & Bussa, T. (2015). Magic quadrant for security information and event management. Gartner Group Research Note.

Kindervag, J. (2010). Build security into your network's dna: The zero trust network architecture. *Forrester Research Inc*, *27*.

Kuzminykh, I., Yevdokymenko, M., & Ageyev, D. (2020). Analysis of encryption key management systems: Strengths, weaknesses, opportunities, threats. In *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)* (pp. 515-520). IEEE

Martins, M. A., & Bruno, L. C. (2022, June). Monitoring Security Risks of Teleworker Devices in Hospital Institution. In *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.

Microsoft (2021) Zero Trust adoption report: How does your organization compare? [Blog post]. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/07/28/zero-trust-adoption-report-how-does-your-organization-compare/

Minnaar, A., & Herbig, F. J. (2021). Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, *34*(3), 155-185.

Plachkinova, M., & Knapp, K. (2022). Least Privilege across People, Process, and Technology: Endpoint Security Framework. Journal of Computer Information Systems, 1-13.

Saeli, S., Bisio, F., Lombardo, P., & Massa, D. (2020). DNS covert channel detection via behavioral analysis: a machine learning approach. *arXiv preprint arXiv:2010.01582*.

Renardi, M. B., Basjaruddin, N. C., & Rakhman, E. (2018). Securing electronic medical record in near field communication using advanced encryption standard (AES). *Technology and Health Care*, *26*(2), 357-362.

Sanders, M. W., & Yue, C. (2019, December). Mining least privilege attribute based access control policies. In *Proceedings of the 35th Annual Computer Security Applications Conference* (pp. 404-416).

Singh, A., Chatterjee, K., & Satapathy, S. C. (2023). TrIDS: an intelligent behavioural trust based IDS for smart healthcare system. *Cluster Computing*, *26*(2), 903-925.

Sisala, S., & Othman, S. H. (2020). Developing a Mobile device management (MDM) security metamodel for bring your own devices (BYOD) in hospitals. *International Journal of Innovative Computing*, *10*(2).

Shahid, A., Nguyen, T. A. N., & Kechadi, M. T. (2021). Big data warehouse for healthcare-sensitive data applications. *Sensors*, *21*(7), 2353.

Sheikh, N., Pawar, M., & Lawrence, V. (2021). Zero trust using network micro segmentation. In *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1-6). IEEE.

Song, H., Fink, G. A., & Jeschke, S. (Eds.). (2017). *Security and privacy in cyber-physical systems: foundations, principles, and applications*. John Wiley & Sons.

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. Digital Health, 9, 20552076231177144.

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.

Tyler, D., & Viana, T. (2021). Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. *Applied Sciences*, *11*(16), 7499.

Vukotich, G. (2023). Healthcare and Cybersecurity: Taking a Zero Trust Approach. *Health Services Insights*, *16*, 11786329231187826. (data breach)

Wani, T. A., Mendoza, A., & Gray, K. (2020). Hospital bring-your-own-device security challenges and solutions: systematic review of gray literature. *JMIR mHealth and uHealth*, *8*(6), e18175.

Yan, X., & Wang, H. (2020). Survey on zero-trust network security. In *Artificial Intelligence and Security: 6th International Conference, ICAIS 2020, Hohhot, China, July 17–20, 2020, Proceedings, Part I 6* (pp. 50-60). Springer Singapore.

Zarate, M. (2021). *Technology Acceptance for Protecting Healthcare Data in the Presence of Rising Secure Sockets Layer/Transport Layer Security Communications: A Generic Qualitative Inquiry* (Doctoral dissertation, Capella University).

.