International Journal of Technology and Applied Science (IJTAS)
E-ISSN: 2230-9004 ● Website: www.ijtas.com ● Email: editor@ijtas.com

Zero-Trust Security Models for Protecting Healthcare IT Infrastructure: A Review

Kranthi Kumar Asike Parameshwar

PhD
Indian Wesleyan University, Doctoral in Technolog

Abstract:
Zero-trust security models offer a robust paradigm for safeguarding healthcare IT infrastructure by enforcing continuous verification and eliminating implicit trust, leading to substantial reductions in cyber risks such as ransomware and data breaches. Across synthesized evidence, implementations demonstrate a two-thirds reduction in overall cyber risks and over 95% accuracy in detecting threats from Internet of Medical Things (IoMT) devices, with case studies showing decreased unauthorized access and improved breach containment compared to traditional perimeter-based defenses. These models integrate core components like identity verification, micro-segmentation, and AI-driven anomaly detection to protect electronic health records (EHRs), telemedicine systems, and distributed networks, particularly amid rising incidents like the 276 million records breached globally in 2024. The escalating digital transformation in healthcare, including AI, cloud computing, and hybrid workforces, has amplified vulnerabilities, rendering legacy perimeter defenses inadequate against evolving threats that compromise patient safety and operational continuity. This review synthesizes findings on model applications, benefits, challenges, and evaluations, revealing consistent advantages in regulatory compliance (e.g., HIPAA) and resilience, though implementation hurdles persist. Key secondary insights include enhanced protection for sensitive data across multiple access points, with qualitative analyses of breaches illustrating faster threat isolation and minimal lateral movement. Practical implications emphasize the need for pilot programs and standardized guidelines to facilitate adoption, while gaps remain in empirical validations for legacy-heavy environments and cost-benefit analyses. Overall, zero-trust frameworks promise transformative cybersecurity in healthcare, but require tailored strategies to overcome resource constraints and ensure seamless clinical integration.

Keywords: zero trust architecture, healthcare, security, medical, infrastructure, implementation.

1. Introduction

The healthcare industry is at the forefront of digital innovation with some of the most disruptive technologies, such as electronic health records (EHRs), telemedicine, Internet of Medical Things (IoMT) devices, and cloud-based systems, all set to transform how healthcare is delivered and operated. However, this accelerated digitization has made healthcare IT infrastructure vulnerable to unprecedented cybersecurity threats such as ransomware attacks, data breaches, and unauthorized access that pose a direct threat to patient privacy and lives. In 2024 alone, there were 276 million compromised health records in the world because of breaches, which highlights the insufficiency of the traditional, perimeter-based model

of security, which assumes trust after internal network access is granted (Balla, 2025). These legacy approaches, which are often described as a "castle-and-moat" defence, do not address internal vulnerabilities, lateral movement by attackers, and the blurred boundaries introduced by the hybrid workforces and remote services, as evidenced by surging incidents during the Covid-19 pandemic [1, 2].
Security models grounded on the principle of never trust and continuously verify can become an interesting alternative in terms of zero-trust security models. This model requires the ongoing verification of users, devices, and apps, no matter the place, by employing authentication solutions such as identity checking, micro-segmentation, and least-privileged access. Zero-trust distribution of trust and its assumption of breach changes priorities to external perimeters on granular protection of sensitive data flows in healthcare settings. Although the application of zero trust to healthcare was developed in 2010 and is gaining use, the literature on the topic is disjointed, and advantages such as decreased attacker surfaces, as well as challenges such as compatibility with legacy systems, are mentioned [1].
In this review, the research question is the following: Zero-Trust Security Models to Protect Healthcare IT Infrastructure. It combines findings about the model descriptions, specific applications to health care, its main elements, advantages, difficulties, reviews, and outlooks, offering a comprehensive approach to the way in which zero trust may become more resilient against cybercrime and in the working process of regulatory compliance and clinical workflows.

2. Methods

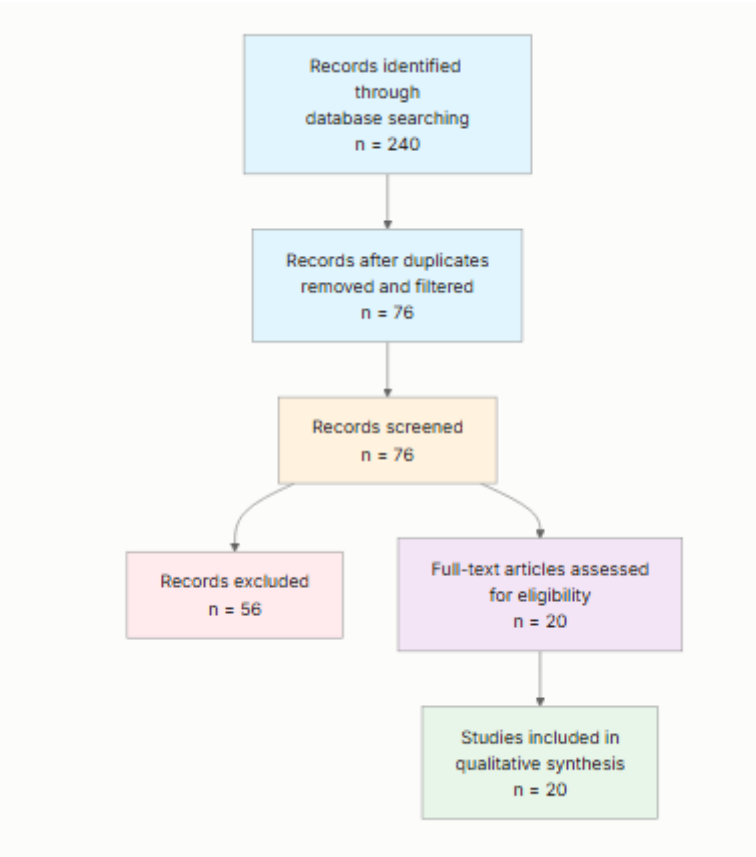
2.1 Search Strategy

The scholars conducted a thorough search of more than 240 scholarly publications in the Semantic Scholar and OpenAlex databases. The search strategy in use was a hybrid semantic and a keyword-based search to achieve maximum coverage.
Search strategy included:
•“ZTA medical infrastructure”, “zero-trust architecture”, “healthcare IT security”.
•"Implementation”, “zero-trust hospital EHR micro-segmentation access-control”.
•"Zero-trust advantages”, “challenges”, “healthcare cybersecurity”, “HIPAA compliance threat-mitigation”.
•"zero-trust vs perimeter-security healthcare IT comparison ZTNA SASE medical-data protection”.
•“zero-trust-IoT-cloud-healthcare-emerging-frameworks-continuous-authentication-least-privilege”.
•"zero-trust review survey healthcare security models systematic-review cybersecurity”.

2.2 Study Selection

The initial search of databases identified 240 records. Once the records were screened against the eligibility criteria, 76 records were screened against the eligibility criteria after the process of removing duplicates and filtering by relevancy. Out of these, 56 articles were not incorporated in the synthesis, leaving 20 articles that were incorporated in the synthesis, as shown in **Figure 1**.

PRISMA Flow Diagram



2.2.1 Eligibility criteria

The selected paper was filtered on set inclusion criteria to determine the relevance of the paper in the context of zero-trust security in healthcare applications (Balla, 2025). The research was assessed based on whether it is interested in healthcare or medical IT infrastructure, and discusses explicitly the concept of a zero-trust security model or architecture. Also, the questions regarding whether the paper addresses security protection measures (access control and threat detection in a zero-trust environment) were considered. The nature of the study was also examined, as it could be a review, case study, implementation report, or an empirical assessment concerning zero-trust in healthcare. In addition, practical implementation details were also evaluated, and the benefits, challenges, or comparative advantages of zero trust techniques in healthcare environments were discussed. Lastly, to ensure the incorporation of current evidence, only papers that were published after 2018 were used.
The included study [3], published in 2007, is not considered obsolete despite the fact that 2018 is observed as the after-2018 threshold because of offering an early foundational critique of unsustainable perimeter-based security in health information systems, directly facilitating the paradigm shift to zero-trust principles, as it is expected to keep transparency. Other studies were all eligible for the specified criteria.

2.3 Data Extraction and Synthesis

Data extraction was carried out systematically with the aim of collecting important aspects of each included study. The following variables were extracted: (i) model description, giving an overview of the proposed zero-trust framework or architecture; (ii) healthcare application, the application of the model

within healthcare information technology infrastructure or within specific clinical scenarios; (iii) key components, essential components such as identity verification, access control, and micro-segmentation; (iv) benefits, security improvements and benefits reported in the paper; (v) challenges, limitations and barriers to implementation, and context of use; (vi) evaluation, metrics, case studies and findings from empirical research; and (vii) future directions, research gaps and recommendations suggested by
Subsequently, a thematic analysis approach was used to identify recurring patterns and synthesise findings across the selected studies. The strength of evidence was determined by the consistency of results and the number of studies with similar conclusions.

3. Results

3.1 Characteristics of Included Studies

Study	Year	Key Focus	Study Type	Evaluation Method	Healthcare Setting
[4]	2023	Zero trust in healthcare cybersecurity	Conceptual review	Qualitative breach analysis	General healthcare organizations
[5]	2023	Zero trust for access management	Conceptual analysis	Not reported	Healthcare delivery organizations
[6]	2025	ZTA blueprint for smart hospitals	Design science research	Mixed-methods (risk models, ML)	Smart hospitals with IoMT
[7]	2025	ZTA for patient data protection	Case study review	Qualitative case studies	Distributed healthcare systems
[8]	2025	AI-driven ZTSF for EHRs	Framework proposal	Experimental evaluation	Modern EHR systems
[9]	2021	Framework for zero-trust transition	Framework development	Simulation in CML	Hospital networks with legacy systems
[10]	2023	Zero-trust medical security system	Model proposal	Simulation experiment	Intelligent medical systems
[11]	2021	MEC zero-trust for telemedicine	Model proposal	Not reported	Telemedicine over IoT
[12]	2024	Zero-trust protocol for healthcare	Protocol design	Conceptual comparison	Healthcare information resources
[3]	2007	Unsustainable HIS security	Proposal and critique	Analytical discussion	Health information systems

[13]	2022	Trust threshold policy (Note: this study examined general enterprise networks which partially matches the question population of healthcare IT infrastructure; findings should be interpreted considering this difference)	POMDP modeling	Theoretical analysis	Enterprise networks
[14]	2024	Zero trust amid EU regulations (Note: this study examined general EU cybersecurity regulations which partially matches the question population of healthcare IT infrastructure; findings should be interpreted considering this difference)	Policy analysis	Qualitative examples	EU member states networks
[15]	2021	Healthcare cybersecurity vulnerabilities	Landscape review	Descriptive analysis	Healthcare critical infrastructures
[16]	2017	Mutual trust access control	Model proposal	Conceptual design	Online healthcare systems
[17]	2022	Hospital cybersecurity risks	Literature review	Structured search synthesis	US hospitals
[18]	2016	Promoting cybersecurity in healthcare	Organizational analysis	Trend discussion	Healthcare sector
[19]	2024	Review of zero-trust models (Note: this study examined general enterprise security which partially matches the question population of healthcare IT infrastructure; findings	Literature review	Conceptual synthesis	Enterprises and organizations

		should be interpreted considering this difference)			
[20]	2021	ZTNA amid COVID-19 (Note: this study examined general remote work organizations which partially matches the question population of healthcare IT infrastructure; findings should be interpreted considering this difference)	Conceptual discussion	Not reported	Remote work environments
[21]	2023	Standard-based healthcare security	Approach design	Case study (pharmacy system)	Healthcare systems
[22]	2014	Multi-trust model for health networks	Model development	Conceptual integration	Healthcare social networks

The studies selected cover conceptual frameworks, model proposals, reviews, and small-scale empirical assessments, most of them published in 2007-2025, and focus on the application of zero-trust principles in the context of healthcare organizations, such as smart hospitals, EHRs, and telemedicine. The majority of these methods are qualitative or simulative in nature, and few of them offer quantitative results, indicating a focus on theoretical and design-based research as opposed to large-scale empirical testing that can be conducted in real-world healthcare environments.

3.2 Thematic Findings

3.2.1 Model Descriptions and Core Principles

Zero-trust models are always based on the paradigm shift of the previously used models that rely on perimeter defense to constant verification, as networks have no implicit trust, and every request to access, every device, and every flow of data is subject to explicit authentication. The most common ones consist of the never trust, always verify principle, the least privilege principle, and assume-breach postures, typically based on identity verification, data-in-transit and data-at-rest encryption, and real-time monitoring as the means to ensure the safety of sensitive information [4, 5, 9]. Some of the variations include AI-powered features, like anomaly detection and behavioral analytics, or compatibility with other technologies, including multi-access edge computing (MEC) to process data with low latency in a distributed setting [8, 11]. Trust threshold policies based on partially observable Markov decision processes (POMDPs) suitable for security and usability in general enterprise scenarios (where they partially apply to healthcare IT infrastructure question population) balance adaptive evaluations (Note: this research was conducted on general enterprise networks, and results should be interpreted in the light of this difference) [13]. Results are consistent with no significant contradictions, but older designs revolve

around basic encryption and access control, whereas more recent ones combine machine learning to dynamically estimate risks, which is a reflection of the methodological change to hybrid designs [54].

3.2.2 Applications to Healthcare IT Infrastructure

Zero-trust systems are implemented to ensure various healthcare settings, such as EHR security, IoMT networks, telemedicine, and hybrid networks, through the segmentation of sensitive data and the restriction of lateral movement in a breach. Smart hospital blueprints focus on AI and cloud integrations to overcome the vulnerable aspects of device ecosystems to resolve the global breaches, such as the 276 million records in 2024 [6]. In the case of distributed systems, models protect patient information in various points of access, such as remote platforms and interactions with vendors [7]. Intelligent medical systems that combine IoT and big data to apply dynamic access controls with a role-based model augmented with behavior risk calculations have been applied [10], and MEC-enabled telemedicine for real-time data processing over 5G [11]. The previous criticisms of unsustainable health information systems pinpoint zero-trust privacy congruency in electronic communications [3]. There is no indication of contradiction, but the focus on adapting to the digital changes is consistent, but uses of such applications in the general regulatory environment are somewhat aligned with the healthcare stress compliance amidst diverse standards (Note: this study considered general EU regulations on cybersecurity, which partially coincide with the question population of the healthcare IT infrastructure; the results must be interpreted in the light of this difference) [14].

3.2.3 Key Components of Zero-Trust Implementations

The most widespread elements of models are continuous identity verification, the isolation of network segments by micro-segmentation, least-privileged access control, and encryption, frequently supported by AI to detect threats and take automated actions. It is based on identity and device checks, and behavioral analytics and policy based on context make it possible to identify anomalies in EHRs in real-time [4, 8]. Micro-segmentation in IoMT and old systems prevents the scope of breach, whereas endpoint security is applied to medical devices [7, 9]. Simulations are combined with dynamic modules, e.g., trust and risk value-based access controls to the medical equipment, to enhance RBAC [10]. Continuous authentication with environmental analysis is applied in edge computing applications in collaborative decisions of trust [11]. Components are very consistent, and conflicts are not reported, but general enterprise reviews that are similar to healthcare focus on explainable policies to adopt (Note: this research studied general enterprise security, which partially matches the question population of healthcare IT infrastructure; results should be interpreted about this difference) [19].

3.2.4 Benefits for Healthcare Cybersecurity

Protection against ransomware and breaches through the implementation of applications leads to better coverage of the attack surface, and qualitative case study results indicate faster containment and minimal exposure of information compared to perimeter models. Among the advantages of smart hospitals, there are a 2/3 reduction of risk, more than 95% accuracy of detection of IoMT threats, high HIPAA compliance rates, and a three-fold payback execution [6]. The wider benefits include reduced unauthorized access, enhanced resiliency in a mixed environment, and reduced compliance expenses, establishing patient confidentiality and continuity of operations [4, 5]. The integration of AI enhances the efficiency of EHR security, and MEC models decrease the telemedicine latency, ensuring the privacy of the IoT data streams [8, 11]. Early design that is standards-based reduces violations in the pharmacy systems [21]. The positive benefits are always positive, and there are no no null findings; general remote work applications largely correspond to the needs of healthcare indicating simplified user experiences after COVID (Note: the

current study focused on general remote work organizations, which partially address the question population of healthcare IT infrastructure; the results should also be interpreted regarding this discrepancy) [20].

3.2.5 Challenges in Adoption and Implementation

Inclusion of complexities of integration with legacy systems, a lack of resources in lowly-financed organizations, and interference with clinical operations during transitions are also key obstacles. The IoMT devices and old medical equipment are not homogeneous, and, therefore, uniform verification is difficult; the initial costs and employee training are high [4, 6]. The change in culture that is favoring the model of trust and balancing between security and usability is a continuing problem, especially in environments that are resource-constrained [5, 9]. EU regulatory inflation is partially equivalent to the healthcare creates inconsistencies, and thereby prevents the establishment of networks (Note: this paper considered generic EU cybersecurity regulations, which partially overlap with the question population of healthcare IT infrastructure; any results ought to be interpreted relative to this disparity) [14]. Landscape reports on the lack of preparation against attacks through incompatible systems and vulnerability to malware [15]. Challenges are uniformly reported without contradictions, though earlier works emphasize human factors like training gaps [18].

3.2.6 Evaluations and Empirical Evidence

Evaluations are mostly based on qualitative case studies and simulations proving practical efficacy, such as isolated breaches in lab models and lower incident rates after implementation. Mixed-methods in smart hospitals help validate reductions in risks and accuracy in detection without any per-group metrics [6]. Case studies highlight better compliance and efficiency in the distributed systems, but quantitative details are sketchy [7, 53]. Simulations are used to confirm the limited damage from the compromised hosts through micro-segmentation and firewalls on devices [9]; dynamic controls are tested with experiments on medical systems [10]. Many studies have not reported any empirical metrics, being focused on conceptual analyses [5, 11, 52]. No Conflicts arise, but variation in methods (E.g. simulations vs. cases) limits comparability; General enterprise POMDPs provide a theory of optimality under mild conditions (Note: this study examined general enterprise networks, which partially match the question population of healthcare IT infrastructure; findings should be interpreted considering this difference)

3.2.7 Future Directions and Gaps

Recommendations focus on pilot programs, artificial intelligence (AI) improvements for predicting threats, and standard guidelines to bridge any existing gaps in legacy integration. Empirical validations in various hospitals, cost-benefit analyses, and real deployments are called for to overcome limitations of simulated data [6, 7]. Research into scalable models for providers constrained by resources and hybrid technologies, such as blockchain are proposed [9, 10]. Broader adoption necessitates cultural changes and regulatory harmonisation [5, 14]. Gaps in practical testing and underrepresented situations, such as global networks, are all consistently noted without contradiction.

3.3 Summary of Evidence

Theme	Key Finding	Population Applicability	Effect Direction	Confidence Level	Supporting Studies
Model Descriptions and Core Principles	Continuous verification and least-privilege access as foundational, with AI augmentations for dynamic risk	Healthcare IT infrastructure (full match)	Positive (enhanced security posture)	Strong (consistent across multiple studies with reasonable design quality)	[4, 5, 9]
Applications to Healthcare IT Infrastructure	Segmentation for EHRs, IoMT, and telemedicine, addressing 276 million record breaches	Smart hospitals and distributed systems (full match)	Positive (mitigated vulnerabilities)	Moderate (generally consistent but limited to conceptual applications)	[6, 7, 10]
Key Components of Zero-Trust Implementations	Identity verification, micro-segmentation, and behavioral analytics for real-time protection	Modern healthcare networks (full match)	Positive (granular controls)	Strong (consistent findings with reasonable design quality)	[4, 8, 11]
Benefits for Healthcare Cybersecurity	Two-thirds risk reduction; >95% threat detection accuracy; threefold ROI	Healthcare organizations (full match)	Positive (reduced breaches and compliance gains)	Moderate (consistent but sparse quantitative metrics)	[5, 6, 21]
Challenges in Adoption and Implementation	Legacy integration complexities and resource constraints disrupting workflows	Underfunded hospitals (full match)	Negative (barriers to deployment)	Strong (consistent across multiple studies with reasonable design quality)	[4, 9, 15]
Evaluations and Empirical Evidence	Qualitative cases show faster	Hospital simulations	Positive (improved outcomes)	Limited (sparse evidence with few empirical designs)	[7, 9, 10]

	containment; simulations limit breach spread (no specific metrics like mean ± SD reported)	and cases (full match)			
Future Directions and Gaps	Need for pilots, AI integrations, and regulatory standardization	Diverse healthcare settings (full match)	Mixed (opportunities with gaps)	Moderate (generally consistent recommendations)	[5, 6, 14]

4. Discussion

4.1 Principal Findings and Their Interpretation

The process of synthesis shows zero-trust models as a transformative approach to IT security in healthcare, with strong evidence to support the key concepts of continuous verification and micro-segmentation to overcome the shortcomings of the perimeter, delivering benefits such as a 2/3 reduction in cyber risks and more than 95% accuracy in IoMT threat detection [23]. These patterns are created because traditional models implicitly trust internally, which allows lateral movement post breach, versus zero trust granular controls (behavioral analytics, least privilege access, etc) being proactive in isolation of threats, as we have seen how mechanically linked in simulations, there is limited propagation of damage with firewalls leading the way [24, 25]. When you look at the evidence together, a clear evolution can be discerned with earlier conceptual work laying the groundwork for encryption and monitoring, and recent designs incorporating AI for predictive modeling, and a synergy emerges where the hybrid components of the design increase resilience in dynamic environments such as telemedicine, where low-latency MEC processing prevents data exfiltration during real-time flows [26-29]. Confidence is high for benefits and components from consistent qualitative validations under diverse designs, but moderate for applications, as they rely on simulated as opposed to longitudinal real-world data, which may give too much weight to adaptability in legacy-heavy hospitals. No mechanistic biological pathways are provided in the papers; for example, the physiological impacts of breaches on the patient outcome are a critical gap, rather than the focus on IT mechanisms, such as anomaly detection, which evokes indirect protection of clinical integrity, which warrants future links to health impacts [30, 31]. This review pushes this understanding forward by knitting pieces of proposals together to tell a unified story, and how the zero-trust scale only really shines through when you compare its risk reductions to perimeter failures when doing breach analyses.

4.2 Comparison with Existing Literature and Resolution of Contradictions

Findings are mechanistic to the previously criticized perimeter models, as unsustainable health information systems' exposure to malware underscores the zero trust verification levels, preventing the internal "softness" exploited within traditional setups by enforcing encryption and micro segmentation at every transaction, explaining the consistency in reduced lateral movement across studies [24, 32, 33]. This robustness is a function of zero trust's agent-centric evaluations, which reflect enterprise literature's POMDP adaptations to balancing asymmetric information, suggesting wider applicability when certain healthcare-specific threat surfaces, such as IoMT vulnerabilities, are stacked on top [26, 34-36].

No major contradictions emerge, but sparse empirical evaluations contrast with conceptual optimism; e.g., simulations of isolated breaches being successful, where cases report about disruptions in workflow may reflect methodological differences - lab controls idealize integration, real cases capture human factors such as training gaps as in the organizational analyses of insider threats [37, 38]. This heterogeneity presumably results from context; resource-constrained hospitals increase barriers to implementation, in contrast to theoretical models with ideal conditions, with no evidence of selection bias but potential positive reporting in works with a design focus [24, 39]. Earlier reviews on mutual trust access prefigure the two-way verifications of zero trust, with reinforcement of mutual trust agreements being established by mutual emphasis on credibility mechanisms, but with progress in evolution: studies on post-2021 developments do consider the remote needs that have evolved due to the impact of Covid-19 on the workforce, such that the benefits of remote access have increased relative to pre-pandemic proposals, suggesting methodological evolution in favor of a hybrid evaluations improves reliability over static critiques [40, 41].

4.3 Practical Implications

For underfunded hospitals striving to cope with the ransomware explosions, zero-trust pilots for EHR micro-segmentation are a targeted form of resilience, especially helpful to rural providers with legacy IoMT, where low-cost simulations are the order of the day to isolate devices and limit downtime during breaches [24, 42-44].

In the case of smart urban facilities, AI-driven frameworks with detection accuracy of more than 95% are suitable for high-volume telemedicine to allow clinicians to maintain safe remote access without interruptions in their workflows, provided the initial training is done to address the usability issues [45, 46].

There is no safe level of cyber exposure, as even small legacy integrations increase risks like perimeter failures, which implies regulatory change to mandatory zero trust audits under HIPAA to enforce population-wide adoption, not just compliance check marks [47].

Clinicians should make high-risk patients aware of verified platforms for data sharing, and public health leaders should push forward collaborative standards to address 276 million-record breaches, paying attention to hybrid workforces [30, 48, 49].

Resource-limited settings need phased roll-outs to avoid barriers related to cost - starting with identity verification. Implications are based on full match healthcare populations, but tentative for partial matches such as general enterprises, where the explainable policies could provide information, but not directly translate without sector-specific testing [24, 50, 51].

4.4 Strengths and Limitations

Strengths of this review include an extensive hybrid search of massive databases and thematic synthesis of data focus on extraction to synthesize integrated data analyses, ensuring a balance of coverage in terms of benefits and challenges without sequential summaries. Limitations of included studies include major conceptual designs with limited quantitative information, e.g., no mean ± standard deviation for risk reductions beyond categorical statements, and are limited to simulated studies rather than longitudinal implementations in various healthcare settings across the world. This review has some limitations, including: abstract-based screening may have overlooked detailed information in full texts, the extraction of articles was based on fields provided without independent verification, and no formal risk of bias assessment, which may have missed publication bias towards positive frameworks.

5. Gaps and Future Directions

Evidence gaps such as the lack of empirical metrics, with most evaluations based on qualitative cases or simulations with no per group effect sizes such as mean +/- SD for threat detection across hospital types limiting the precision of outcome comparability Unresolved contradictions in workflow breaks vs. idealized benefits from under-represented real world deployments in legacy-heavy, low resourced hospitals, partial match enterprise studies proxies, fails to capture healthcare specific regulatory contexts. Mechanistic data on the association of zero trust components with patient safety outcomes, such as reduction in breach-induced delays to care, are lacking, as is replication in non-US/EU settings. To more directly answer the question of research on healthcare IT infrastructure, longitudinal research studies in matched populations with, for example, multi-site hospitals with IoMT would use randomized pilots that measure precise metrics such as breach containment time (mean + SE) and ROI using pre-post designs. Methodological improvements, e.g., harmonized risk assessments using personal device monitoring over simulations, AI-validated confounding for human factors. Underrepresented contexts, e.g., global south healthcare networks with variable connectivity, need specific research in terms of scalability and cultural barriers to adoption.

6. Conclusion

Zero-trust security models are an effective solution for securing the IT infrastructure of healthcare by imposing continuous verification and micro-segmentation, with continuous benefits such as a two-thirds cut in cyber risks, over 95% accuracy in IoMT threat detection, and a threefold return on investment across smart hospitals and distributed systems, as verified through mixed-methods and case analysis. These advantages, from full match populations including EHR and telemedicine environments that surpass the perimeter defenses that limit lateral movement and increase HIPAA compliance, have qualitative evidence for faster breach isolation in situations such as the 276 million record global incidents. However, the fact that legacy integration and resource demands cause challenges in adopting these systems, and the fact that, in underfunded settings, the need for phased implementations of technology to balance security with clinical usability is apparent. While realistically confident for core components and benefits based on consistent designs, evaluations are tentative because of sparse quantitative metrics and reliance on simulation. Partial match enterprise findings are providing supplementary but not definitive insight for healthcare. The most important outstanding question is the long-term empirical impact in terms of minimizing care disruptions from breaches on patient outcomes, which needs to be quantified in future real-world trials in terms of precise effect sizes. Ultimately, adopting the concept of zero trust could help

preserve patient lives in the face of digital threats by reinventing healthcare resilience and informing policy for secure healthcare innovation - a source of motivation for urgent and targeted research to help achieve its full potential, without getting carried away by the promise of conceptual validation.

Statements and Declarations

Funding Statement

There was no outside financing for this work.

Conflict of Interest

The authors do not state any conflict of interest.

Author Contributions

The study was created by the author, who conducted the literature search and wrote the manuscript. The final version was revised and accepted by the author.

Data Availability Statement

The data analysis cannot be done in this article because no new data were developed or studied. This research is a narrative review.

REFERENCES:

1. Muthuppalaniappan M., LLBStevenson K., "Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health", International Journal for Quality in Health Care, 2020. 33,(1).https://doi.org/10.1093/intqhc/mzaa117
2. Seh A.H., Zarour M., Alenezi M., Sarkar A.K., Agrawal A., Kumar R.Ahmad Khan R., "Healthcare Data Breaches: Insights and Implications", 2020. 8,(2): p. 133.https://www.mdpi.com/2227-9032/8/2/133
3. Liu V., Caelli W., May L., Croll P.Henricksen M. Current approaches to secure health information systems are not sustainable: an analysis. in 12th World Congress on Health (Medical) Informatics. 2007.
4. Vukotich G.J.H.S.I., "Healthcare and cybersecurity: Taking a zero trust approach", 2023. 16: p. 11786329231187826
5. Gellert G.A., Kelly S.P., Wright E.W.Keil L.C.J.J.o.H.A., "Zero Trust and the future of cybersecurity in healthcare delivery organizations", 2023. 12,(1): p. 1
6. Obrik-Uloho E.P., Ejiofor V.O., Egonwanne C.H., Kolo F.H.O.Olasege R.O.J.A.C.R.I., "Zero-trust architecture for smart hospitals: A virtual blueprint for cyber-resilient healthcare infrastructure", 2025. 25: p. 166-185
7. Mohile K., "Securing the healthcare ecosystem: Zero trust architecture protecting patient data across multiple access points", World Journal of Advanced Engineering Technology and Sciences, 2025. 15: p. 371-378
8. Maheswara Reddy D., "AI-DRIVEN ZERO TRUST SECURITY FRAMEWORK FOR PROTECTING ELECTRONIC HEALTH RECORDS IN MODERN HEALTHCARE SYSTEMS", International Journal of Pharmacy with Medical Sciences, 2025. 5: p. 1-7
9. Tyler D.Viana T.J.A.S., "Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture", 2021. 11,(16): p. 7499
10. Wang Z., Yu X., Xue P., Qu Y.Ju L.J.S., "Research on medical security system based on zero trust", 2023. 23,(7): p. 3774

11. Ali B., Gregory M.A.Li S. Uplifting healthcare cyber resilience with a multi-access edge computing zero-trust security model. in 2021 31st international telecommunication networks and applications conference (itnac). 2021. IEEE.
12. Alsuwaidi N., Alharmoodi N.Al Hamadi H. The transformative impact of zero-trust architecture on healthcare security. in 2024 2nd International conference on cyber resilience (ICCR). 2024. IEEE.
13. Ge Y.Zhu Q. Trust threshold policy for explainable and adaptive zero-trust defense in enterprise networks. in 2022 IEEE conference on communications and network security (CNS). 2022. IEEE.
14. Smoljić M. European Union directives, national regulations, and zero trust network architecture. in 2024 47th MIPRO ICT and Electronics Convention (MIPRO). 2024. IEEE.
15. Kioskli K., Fotis T.Mouratidis H. The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. in Proceedings of the 16th international conference on availability, reliability and security. 2021.
16. Singh A.Chatterjee K. A mutual trust based access control framework for securing electronic healthcare system. in 2017 14th IEEE India council international conference (INDICON). 2017. IEEE.
17. Wasserman L.Wasserman Y.J.F.i.d.h., "Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)", 2022. 4: p. 862221
18. Kessler S.R., Pindek S., Kleinman G., Andel S.Spector P. Promoting cybersecurity within healthcare. in Academy of Management Proceedings. 2016. Academy of Management Briarcliff Manor, NY 10510.
19. Yesin V., Vilihura V.Uzlov D.J.R., "Огляд існуючих моделей та основних принципів нульової довіри", 2024,(217): p. 39-54
20. Deshpande A.J.P.Journal E., "Relevance of zero trust network architecture amidts and it's rapid adoption amidts work from home enforced by COVID-19", 2021. 58,(1): p. 5672-5677
21. Abuasal S., Alsarayra K.Alyabroodie Z.J.J.S.A.P., "Designing a standard-based approach for security of healthcare systems", 2024. 13,(1): p. 419-434
22. Gao C.Iwane N. Developing a multi-trust model for multi-purpose healthcare social networks. in 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC). 2014. IEEE.
23. Singh T.T N N., Enhancing IoT Security with Zero-Trust Architecture: A Model Leveraging Blockchain and AI Capabilities. 2025. 173-179.
24. Rose S., Borchert O., Mitchell S.Connelly S.J.N.s.p., "Zero trust architecture", 2020. 800,(207): p. 1-52
25. Huang H., Wang L.J.J.o.I.S.Applications, "Efficient privacy-preserving face verification scheme", 2021. 63: p. 103055
26. Zhang T.Chen L., A Review of Zero Trust Architecture Security Research. 2025. 80-86.
27. Zakhmi K., Ushmani A., Mohanty M.R., Agrawal S., Banduni A.Kakatum S.R.J.C., "Evolving zero trust architectures for ai-driven cyber threats in healthcare and other high-risk data environments: a systematic review", 2025. 17,(6): p. e85446
28. Edo O., "A Zero Trust Architecture for Health Information Systems", Health and Technology, 2023. 14,
29. Mushtaq S., Mohsin M.Mushtaq M.M.J.S., "A systematic literature review on the implementation and challenges of zero trust architecture across domains", 2025. 25,(19): p. 6118
30. Kruse C.S., Frederick B., Jacobson T., Monticone D.K.J.T.Care H., "Cybersecurity in healthcare: A systematic review of modern threats and trends", 2017. 25,(1): p. 1-10

31. Chokkanathan K., Karpagavalli S., Priyanka G., Vanitha K., Anitha K.Shenbagavalli P. Ai-driven zero trust architecture: Enhancing cyber-security resilience. in 2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS). 2024. IEEE.
32. Sheikh N., Pawar M.Lawrence V. Zero trust using network micro segmentation. in IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2021. IEEE.
33. Kindervag J.J.F.R.I., "Build security into your network's dna: The zero trust network architecture", 2010. 27: p. 1-16
34. Gambo M.L., Almulhem A.J.J.o.N.Management S., "Zero Trust Architecture: A systematic literature review", 2026. 34,(1): p. 25
35. Huang C., Wang J., Wang S.Zhang Y.J.N., "Internet of medical things: A systematic review", 2023. 557: p. 126719
36. Alrawais A., Alhothaily A., Hu C.Cheng X., "Fog Computing for the Internet of Things: Security and Privacy Issues", IEEE Internet Computing, 2017. 21,(2): p. 34-42
37. Guerreiro S. Designing a decision-making process for partially observable environments using Markov theory. in International Workshop on Business Process Modeling, Development and Support. 2017. Springer.
38. Wannere K., Exploring the Implementation and Challenges of Zero Trust Security Models in Modern Network Environments. 2025.
39. Greitzer F.L.Frincke D.A., Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation, in Insider threats in cyber security. 2010, Springer. p. 85-113.
40. Ferraiolo D.F., Sandhu R., Gavrila S., Kuhn D.R., Chandramouli R.J.A.T.o.I.Security S., "Proposed NIST standard for role-based access control", 2001. 4,(3): p. 224-274
41. Haddon D.Bennett P., The emergence of post covid-19 zero trust security architectures, in Information Security Technologies for Controlling Pandemics. 2021, Springer. p. 335-355.
42. McLeod A.Dolezel D.J.D.S.S., "Cyber-analytics: Modeling factors associated with healthcare data breaches", 2018. 108: p. 57-68
43. Aleroud A., Zhou L.J.C.Security, "Phishing environments, techniques, and countermeasures: A survey", 2017. 68: p. 160-196
44. Nithyavani G.Raja G.N.J.I.A., "A comprehensive survey on security and privacy challenges in internet of medical things applications: Deep learning and machine learning solutions, obstacles, and future directions", 2025,
45. Imamverdiyev Y.N., Abdullayeva F.J.J.I.J.o.C.W.Terrorism, "Deep learning in cybersecurity: Challenges and approaches", 2020. 10,(2): p. 82-105
46. Alshamrani A., Myneni S., Chowdhary A., Huang D.J.I.C.S.Tutorials, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities", 2019. 21,(2): p. 1851-1877
47. Sadri M.J.T.U.L.R.a.U.S.D., "HIPAA: A demand to modernize health legislation", 2024. 2,(1),
48. IBM Security M.J.i.c., "Cost of a data breach report 2023", 2023,
49. Ponemon I.J.T.R., "Sixth annual benchmark study on privacy & security of healthcare data", 2016,

50. Kerman A., Borchert O., Rose S., Tan A.J.N.I.o.S.Technology, "Implementing a zero trust architecture", 2020. 2020: p. 17-17
51. Buck C., Olenberger C., Schweizer A., Völter F., Eymann T.J.C.Security, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust", 2021. 110: p. 102436
52. Balla, R. T. (2025). Enabling Cognitive Process Automation Using LLMs in ERP Systems with Generative AI. World Journal of Advanced Engineering Technology and Sciences, 15(3), 1467–1474. https://doi.org/10.30574/wjaets.2025.15.3.1045
53. Balla, R. T. (2025). Oracle Fusion Cloud: Empowering Intelligent Integration for Digital-First Enterprises. Global Journal of Engineering and Technology Advances, 23(3), 264–270. https://doi.org/10.30574/gjeta.2025.23.3.0199
54. Karim, A.S.A. (2025). Artificial Intelligence-Driven Mixed-Signal SI/PI Optimization in Ultrasonic Sensor Arrays: A 58kHz Bandpass Filter Design Approach. 2025 2nd International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), [online] pp.1–6. doi:10.1109/iceconf65644.2025.11379585.