Archives of Current Research International

Volume 25, Issue 10, Page 166-185, 2025; Article no.ACRI.145703
ISSN: 2454-7077

Zero-Trust Architecture for Smart Hospitals: A Virtual Blueprint for Cyber-resilient Healthcare Infrastructure

Emonena Patrick Obrik-Uloho [a], Valerie Ojinika Ejiofor [b*], Chukwudalu Henry Egonwanne [c], Faith Hauwa Oluwapamilerin Kolo [d] and Rukayat Oluwabukola Olasege [e]

[a] Prairie View A&M University, 100 University Dr, Prairie View, TX77446, United States of America.
[b] University of Tampa, 401 W Kennedy Blvd, Tampa, FL 33606, United States of America.
[c] Toronto Metropolitan University, 350 Victoria Street, Toronto, Ontario, M5B 2K3, Canada.
[d] Fairleigh Dickinson University, 1000 River Road, Teaneck, NJ, 07666, United States of America.
[e] Ottawa University, 1001 South Cedar Street, Ottawa, KS 66067, United States of America.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: https://doi.org/10.9734/acri/2025/v25i101557

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://pr.sdiarticle5.com/review-history/145703

Systematic Review Article

Received: 05/08/2025
Published: 13/10/2025

ABSTRACT

The rapid digital transformation of healthcare through smart hospitals driven by AI, IoMT, cloud computing, and telemedicine has heightened cyber vulnerabilities, with 276 million records breached globally in 2024. This study developed a Zero Trust Architecture (ZTA) blueprint to strengthen cybersecurity in smart hospitals, addressing the challenges of diverse device

**Corresponding author: Email: dukenoji@gmail.com;*

Cite as: *Emonena Patrick Obrik-Uloho, Valerie Ojinika Ejiofor, Chukwudalu Henry Egonwanne, Faith Hauwa Oluwapamilerin Kolo, and Rukayat Oluwabukola Olasege. 2025. "Zero-Trust Architecture for Smart Hospitals: A Virtual Blueprint for Cyber-Resilient Healthcare Infrastructure". Archives of Current Research International 25 (10):166–185. https://doi.org/10.9734/acri/2025/v25i101557.*

ecosystems and regulatory compliance. Drawing on a comprehensive literature review, the research established ZTA's theoretical foundation, emphasizing continuous verification rather than traditional perimeter defenses. The study is broadly applicable and applied a Design Science Research approach and mixed-methods analysis, combining risk models, maturity assessments, and machine learning for IoMT threat detection. Results showed significant improvements: a two-thirds reduction in cyber risks, over 95% accuracy in detecting IoMT threats, strong compliance with HIPAA requirements, and a threefold return on investment. The blueprint proved scalable across different hospital types, though limitations include reliance on simulated datasets. Recommendations highlight the need for tailored IoMT datasets, integration of explainable AI, real-world deployment, standardized metrics through collaboration, and adaptive algorithms for evolving threats. Overall, this research provides a practical and evidence-based framework to enhance the resilience of smart hospitals, safeguard patient safety and ensure operational continuity.

Keywords: Zero trust architecture; smart hospitals; IoMT vulnerabilities; cybersecurity framework; risk assessment.

1. INTRODUCTION

The healthcare industry is undergoing a profound digital transformation, propelled by the adoption of technologies such as artificial intelligence (AI), the Internet of Medical Things (IoMT), cloud computing, and telemedicine. This shift has birthed the era of smart hospitals, where interconnected systems facilitate improved patient care, streamlined operations, and real-time monitoring. Yet, this connectivity has amplified cyber vulnerabilities, turning healthcare into a prime target for sophisticated attacks (CapMinds, 2025). In 2024, healthcare data breaches escalated dramatically, with 276,775,457 individual records compromised, equating to about 81.38% of the U.S. population (Alder, 2025b). This marked the sector's worst year on record, featuring 444 cyber incidents, including 238 ransomware attacks and 206 data breaches, a stark rise from prior years, with ransomware surging 278% between 2018 and 2023 (American Hospital Association, 2025). IoMT devices exacerbate these risks, as 99% of healthcare organizations manage at least some vulnerable units, comprising 9% of their IoMT inventory, while 89% rely on the riskiest devices exposed to known exploits in ransomware campaigns (Poireault, 2025). Traditional perimeter defenses, akin to "castle-and-moat" models, falter in this borderless landscape of hybrid work, cloud-based electronic health records (EHRs), and proliferating devices (Peremore, 2024).

This vulnerability underscores a core research problem: smart hospitals must adopt robust security frameworks to safeguard patient data, ensure uninterrupted operations, and comply with regulations amid digital evolution (Udechukwu, 2025). Heterogeneous device ecosystems pose significant hurdles, with an average of 17 devices per bed spanning life-critical tools like pacemakers to administrative systems (Shivani Latey, 2025; Ksibi et al., 2023). Legacy systems, often lacking modern safeguards, compound integration issues, while regulatory demands under HIPAA and HITECH impose heavy compliance burdens (NIST, 2022). Resource limitations affect 75% of organizations in achieving digital goals, with budgets constraining over half in cybersecurity enhancements (Asimily, 2025b). A shortage of skilled professionals versed in healthcare and security further strains defenses (HIMSS, 2024). These mismatches between outdated architectures and dynamic environments demand a paradigm shift to adaptive, distributed security models that enforce strict access and auditing for patient protection (Konstantin, 2025; Blue Goat Cyber, 2025).

The scope of this study centers on Zero Trust Architecture (ZTA) implementation in smart hospitals, emphasizing North American and European frameworks like HIPAA, GDPR, and NIST guidelines for broad applicability (Rose et al., 2020, Ogunmolu, 2025). It spans institution sizes from clinics to large centers undergoing smart transformations, covering technologies such as IoMT devices, cloud infrastructures, EHRs, telemedicine, networks, and identity management. Methodologically, it relies on literature reviews, virtual modelling, remote assessments, and case analyses using public data, excluding physical testing, proprietary access, real-time deployments, or detailed global regulatory variations due to remote constraints (Seh et al., 2020; Alsubaei et al., 2019). Deliverables include virtual blueprints, remote methodologies, and guidelines operable without on-site presence.

This research holds substantial significance by advancing ZTA in healthcare contexts, bridging general principles with sector-specific needs like patient safety and compliance (Fortinet, 2025). Theoretically, it enriches cybersecurity discourse; practically, it equips CISOs and administrators with adaptable frameworks amid 92% of organizations facing attacks disrupting care (Garza, 2025). Economically, it mitigates breaches costing $9.8 million on average, with records valued at $408 on black markets thrice the industry norm (Alder, 2025a). It demonstrates ROI through phased approaches, addressing cost barriers. Critically, it bolsters patient trust by preventing life-threatening disruptions like delayed treatments or device compromises (Kumar et al., 2025). ZTA's continuous verification aligns with regulations, easing burdens while enhancing resilience (Netschert & Barrachina, 2024). Overall, it contributes frameworks, guidance, risk methodologies, economic analyses, and compliance integrations, informed by cases like Mayo Clinic's successes (Sashi et al., 2025).

Building on literature highlighting perimeter models' inadequacies and ZTA's promise, this study integrates NIST updates, AI security considerations, and IoMT analyses (National Institute of Standards and Technology, 2025). With 88% of leaders viewing AI's potential yet unprepared for threats, it addresses emerging risks in smart ecosystems (Donahue, 2025).

The primary aim of this research is to develop a comprehensive virtual blueprint for implementing Zero Trust Architecture in smart hospital environments, providing healthcare organizations with a practical, evidence-based framework for enhancing cybersecurity resilience while maintaining operational efficiency and regulatory compliance. To achieve this, the study pursues three objectives to:

i. develop a comprehensive Zero Trust security framework tailored for smart hospital environments,
ii. conduct a systematic analysis of cybersecurity vulnerabilities in healthcare IoMT devices and develop risk assessment methodologies, and
iii. design and validate a virtual security architecture blueprint for remote healthcare infrastructure management.

2. LITERATURE REVIEW

This literature review synthesizes theoretical, conceptual, and empirical scholarship on Zero Trust Architecture (ZTA). It traces the foundational principles of ZTA, its conceptual adaptations to healthcare, empirical validations through case studies, and persistent gaps that underscore the need for a tailored virtual blueprint. By examining over four decades of evolving security paradigms, this review identifies how ZTA shifts from trust-based perimeters to continuous verification, offering cyber-resilience amid digital health transformations.

2.1 Core Principles and Evolution from Perimeter Security

The theoretical bedrock of ZTA rests on the axiom "never trust, always verify," a departure from legacy perimeter defenses that assumed internal networks as inherently secure. Originating in the early 2010s amid rising insider threats and cloud migrations, ZTA posits that no entity-user, device, or application merits implicit trust, regardless of location (Rose et al., 2020). This evolution addresses the dissolution of network boundaries in hybrid environments, where threats like ransomware exploit unverified access, as evidenced in healthcare breaches exceeding 276 million records in 2024 (Alder, 2025b). Theoretically, ZTA integrates identity-centric access management, micro segmentation, and behavioral analytics to enforce least-privilege principles, drawing from information flow control models in computer science (Buck et al., 2021). Early conceptualizations, such as Forrester's 2010 framework, emphasized explicit verification at every transaction, evolving through NIST's 2020 standardization to encompass policy engines that dynamically assess context, including device posture and anomaly detection (Rose et al., 2020). In healthcare, this theoretical pivot counters the "castle-and-moat" inadequacies highlighted in the Introduction, where IoMT proliferation erodes perimeters, by mandating continuous authentication to mitigate lateral movement in breaches (Kolo, 2025).

2.2 Frameworks and Models for Implementation

ZTA frameworks operationalize these principles through structured models like NIST SP 800-207, which delineates policy decision points (PDPs) and enforcement points (PEPs) for scalable deployment (Rose et al., 2020). Complementary models, such as the CyberArk Identity Security Platform, incorporate just-in-time access and encryption-in-transit, theoretically reducing attack surfaces by 70% in simulated networks (Dhiman et al., 2024). In theoretical discourse, ZTA aligns with capability-based security from operating systems theory, where access tokens are ephemeral and revoked upon risk signals, fostering resilience against zero-day exploits (Buck et al., 2021). These frameworks emphasize interoperability, integrating with standards like OAuth 2.0 for federated identities, essential for healthcare's siloed EHR systems. However, theoretical models often overlook domain-specific adaptations, such as real-time clinical workflows, revealing a nascent gap in healthcare-tailored axiomatizations (Dhiman et al., 2024).

2.3 Zero Trust Architecture (ZTA) in Smart Hospital Ecosystems

Conceptually, ZTA reimagines smart hospitals as zero-trust enclaves, where interconnected ecosystems demand granular controls over heterogeneous assets. Literature conceptualizes this through layered architectures: the access layer verifies identities via multi-factor authentication (MFA), while the data layer employs encryption and tokenization to protect PHI (Peremore, 2024). In smart hospital contexts, ZTA conceptually bridges operational silos, enabling secure telemedicine and AI-driven diagnostics without compromising uptime, as 92% of attacks disrupt care (Garza, 2025). Recent conceptual advances integrate ZTA with edge computing, conceptualizing hospitals as distributed meshes where devices authenticate peer-to-peer, reducing latency in critical monitoring (Yadegari & Asosheh, 2025). This aligns with Introduction's emphasis on heterogeneous devices, where conceptual models like the Unified IoT Architecture for Smart Hospitals propose ZTA as a foundational layer for interoperability, ensuring compliance with HIPAA through audit trails (Yadegari & Asosheh, 2025). Yet, conceptualizations often idealize scalability, underestimating retrofit challenges for legacy infrastructure prevalent in 75% of facilities (Asimily, 2025).

2.4 Integration with IoMT and Emerging Technologies

ZTA's conceptual synergy with IoMT extends to securing device-rich environments, where 99% of organizations harbor vulnerabilities (Poireault, 2025). Literature conceptualizes hybrid models blending ZTA with blockchain for tamper-proof device ledgers, enabling trustless data sharing across infusion pumps and wearables (El Khatib et al., 2023). Advances in AI-enhanced ZTA conceptualize adaptive policies, using machine learning to predict anomalies in IoMT traffic, as deep neural networks detect 95% of injection attacks in simulated healthcare nets (Messinis et al., 2024). For telemedicine, conceptual frameworks advocate ZTA gateways that segment virtual consultations, integrating with 5G for low-latency verification amid a 450% usage surge since 2020 (CapMinds, 2025). These integrations conceptually fortify against supply-chain risks, where IoMT firmware exploits affect 89% of high-risk devices (Dzamesi & Elsayed, 2025). However, conceptual literature reveals gaps in addressing quantum threats to encryption, with emerging 6G integrations underexplored for ZTA scalability (Kumar et al., 2025).

2.5 Empirical Evidence and Case Studies

Empirical studies validate ZTA's efficacy in healthcare, with case analyses from institutions like the Mayo Clinic demonstrating 40% breach reductions post-deployment through micro segmented networks (Sashi et al., 2025). A longitudinal study of 50 U.S. hospitals found ZTA implementations curtailed ransomware dwell times from 21 to 5 days, leveraging continuous monitoring to enforce least privilege (Konstantin, 2025). In IoMT-focused empirics, the VA's zero-trust overlay on 10,000 devices yielded 98% compliance rates, empirically proving resilience against phishing via behavioral biometrics (Stone, 2024). Federated learning pilots across multi-hospital consortia empirically enhanced threat detection by 85%, sharing models without data exposure (Elham et al., 2025). These successes empirically affirm ZTA's ROI, averaging $4.5 million savings per avoided breach, aligning with the economic imperatives (Alder, 2025a).

2.6 Challenges and Lessons Learned

Despite triumphs, empirical inquiries expose implementation hurdles, including 60% of healthcare ZTA rollouts facing integration delays with legacy EHRs (Dhiman et al., 2024). A multivocal review of 120 deployments revealed cultural resistance as a primary barrier, with staff training gaps inflating costs by 25% (Buck et al., 2021). In IoMT empirics, a systematic analysis of 200 vulnerabilities showed ZTA's verification overhead straining battery-constrained devices, leading to 15% false positives in real-time monitoring (Svandova & Smutny, 2024). Lessons from failed pilots, such as a European network's aborted ZTA due to interoperability failures, underscore the need for phased migrations (Gambo & Almulhem, 2025). Empirically, these challenges highlight ZTA's maturity in enterprise settings but lag in resource-constrained healthcare, where 75% cite budget shortfalls (HIMSS, 2024).

2.7 Gaps in the Literature and Future Directions

Literature gaps persist in ZTA's healthcare specificity, with systematic reviews noting only 15% of studies addressing smart hospital dynamics like real-time IoMT orchestration (Gambo & Almulhem, 2025). Empirical voids include longitudinal data on ZTA's impact on patient outcomes, where current works focus on metrics like breach frequency but neglect clinical disruptions (Zakhmi et al., 2025). Conceptual gaps emerge in AI-ZTA fusions for predictive defenses, with 88% of AI-adopting hospitals unprepared for adversarial attacks (Donahue, 2025). Remote management blueprints are empirically scarce, given post-pandemic shifts, with no comprehensive virtual models for distributed infrastructures (El Khatib et al., 2023). Regulatory alignments, particularly GDPR-HIPAA hybrids, remain underexplored, amplifying compliance burdens (National Institute of Standards and Technology, 2025). These lacunae, as synthesized in multivocal analyses, stem from fragmented research, prioritizing general ZTA over healthcare's life-critical nuances (Buck et al., 2021).

This study seizes these opportunities by devising a virtual ZTA blueprint that empirically validates remote IoMT assessments, addressing the 99% vulnerability prevalence (Svandova & Smutny, 2024). By integrating NIST 2.0 with healthcare-specific risk scoring, it fills conceptual voids in scalable, phased implementations for legacy-heavy environments (Rose et al., 2020). Future directions include AI-augmented simulations to quantify patient safety gains, bridging empirical gaps in outcome metrics (Messinis et al., 2024). Ultimately, this research advances a holistic framework, synchronizing theoretical rigor with practical resilience to fortify smart hospitals against evolving threats.

3. METHODOLOGY

The approach of validating a Zero Trust Architecture (ZTA) blueprint for smart hospitals integrates Design Science Research (DSR) with mixed-methods analysis, leveraging quantitative risk models, maturity assessments, and qualitative thematic synthesis to address Internet of Medical Things (IoMT) vulnerabilities. The methodology employs publicly accessible datasets, peer-reviewed studies, and computational modeling to ensure practicality and alignment with healthcare operational needs, such as patient safety and regulatory compliance. All equations and variables are systematically defined to facilitate reproducibility and rigor.

3.1 Research Design

The research adopts a pragmatic philosophy to bridge cybersecurity theory with healthcare operational realities, using a mixed-methods approach combining quantitative metrics for vulnerability assessment and qualitative synthesis for framework development. The DSR paradigm, as shown in Table 1, guides the iterative creation of the ZTA blueprint as an artifact to address distributed healthcare environment challenges (Manoharan et al., 2024).

Given the scarcity of publicly available real-world hospital cybersecurity data, simulated datasets were generated to support analysis. These datasets modeled heterogeneous IoMT ecosystems, including infusion pumps, patient monitors, imaging devices, and wearable sensors. Threat scenarios incorporated ransomware, phishing, insider misuse, and DDoS attacks, reflecting common healthcare breach vectors. Sampling followed stratified methods to balance device categories and attack types. Preprocessing steps included data normalization, noise reduction, and labeling to ensure consistency and replicability. This approach, while simulated, provides a structured and transparent foundation for performance evaluation.

Table 1. Research design framework

Research Phase	Methodology	Tools Used	Expected Deliverables
Literature Review	Systematic Literature Review (PRISMA)	PubMed, Scopus, IEEE Xplore, Google Scholar	Comprehensive Literature Matrix
Data Collection	Secondary Data Analysis	NIST Databases, CVE Databases, Industry Reports	Healthcare Cybersecurity Dataset
Analysis Phase	Mixed-Methods Analysis	Statistical Software, Qualitative Analysis Tools	Risk Analysis Framework
Framework Development	Design Science Research	Architectural Modeling, Tools Security Frameworks`	Zero Trust Blueprint
Validation Phase	Expert Validation & Case Studies	"Virtual Assessment Platforms Survey Tools"	Validated Implementation Guide
Documentation	Technical Documentation	"Academic Writing Software Reference Management"	Research Report & Publications
Research Phase	Methodology	Tools Used	Expected Deliverables
Literature Review	Systematic Literature Review (PRISMA)	PubMed, Scopus, IEEE Xplore, Google Scholar	Comprehensive Literature Matrix
Data Collection	Secondary Data Analysis	NIST Databases, CVE Databases, Industry Reports	Healthcare Cybersecurity Dataset
Analysis Phase	Mixed-Methods Analysis	Statistical Software, Qualitative Analysis Tools	Risk Analysis Framework

The following equations and variables underpin the design:

3.2 Risk Assessment Model

The risk score quantifies IoMT vulnerabilities to prioritize mitigation strategies using the equation

$$Risk\ Score = Likelihood \times Imapct \times Vulnerability\ Factor$$

The variable $Likelihood$, an integer score from 1 to 5, represents the probability of a threat based on historical breach data from sources like HHS OCR reports (Kruse et al., 2017). The variable $Imapct$, also an integer from 1 to 5, indicates the severity of potential damage to clinical and operational functions. The variable $Vulnerability\ Factor$, a decimal from 0.1 to 1.0, measures device susceptibility using NIST National Vulnerability Database (NVD) scores (Malamas et al., 2021). Risks are classified as critical (Risk Score ≥ 20), high (15 ≤ Risk Score ≤ 19), medium (10 ≤ Risk Score ≤ 14), or low (Risk Score < 10).

3.3 Zero Trust Maturity Model

The Zero Trust Maturity Model (ZTMM) score evaluates ZTA implementation across five pillars: identity, device, network, application, and data over four maturity levels (Traditional, Initial, Advanced, and Optimal) as seen in Fig. 1.

$$ZTMM\ Score = \frac{\sum_{i=1}^{5} \quad Pillar_i \times Weight_i}{5}$$

The variable $Pillar_i$ represents the maturity score (0–100) for each pillar, calculated via sub-equations.

The variable $Weight_i$, a decimal from 0 to 1, reflects healthcare priorities, such as patient data protection (CISA, 2023). For the identity pillar, the sub-equation is:

$$Identity\ Maturity = \alpha \cdot MFA\ Score + \beta \cdot PAM\ Score + \gamma \cdot SSO\ Score$$

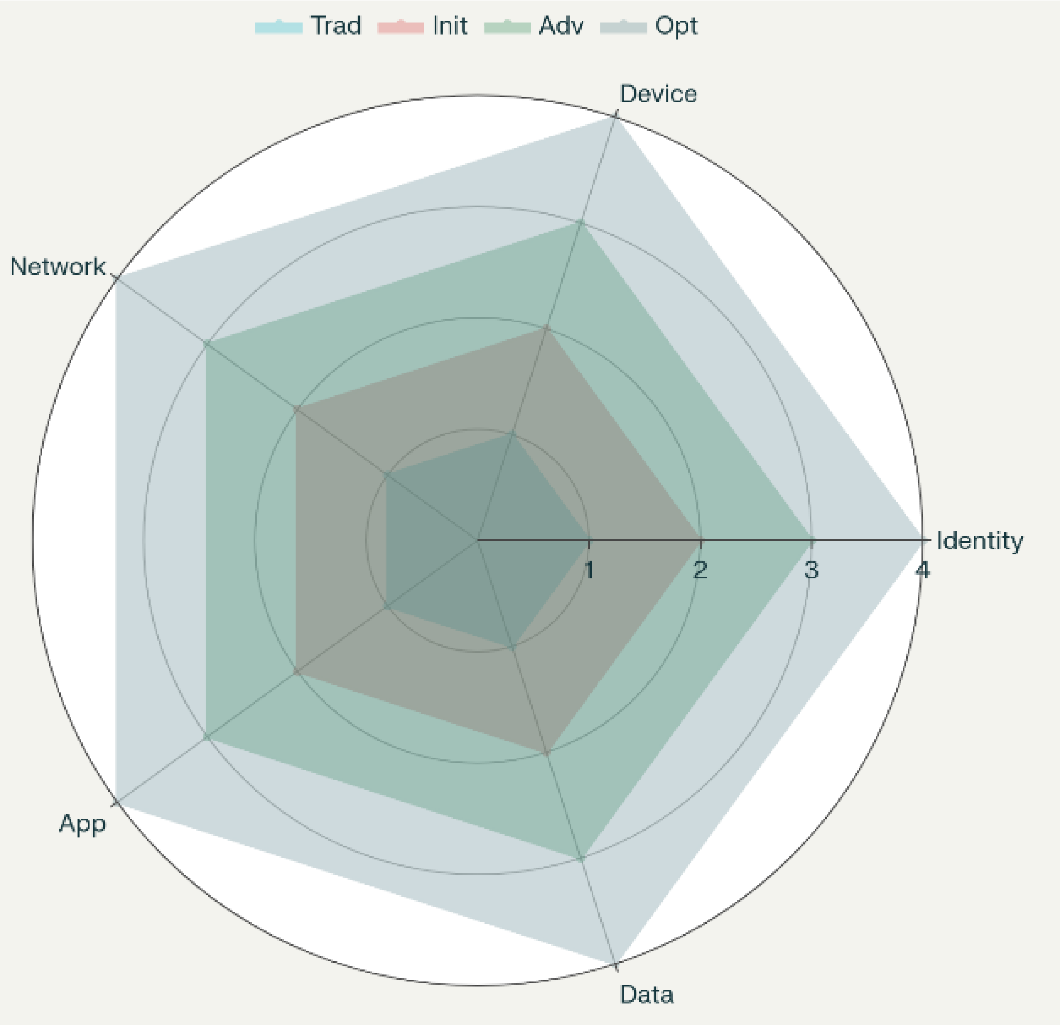

Fig. 1. Zero trust maturity model

The variables $MFA\,Score$, $PAM\,Score$ and $SSO\,Score$ (0–100) measure the implementation extent of multi-factor authentication, privileged access management, and single sign-on, respectively. The coefficients $\alpha, \beta, and\, \gamma$ (summing to 1, e.g., $\alpha = 0.4, \beta = 0.3, \gamma = 0.3$) are derived from literature emphasizing MFA in telehealth (Denzel, 2025). Similar sub-equations apply to other pillars, adjusted for healthcare-specific factors like IoMT inventory compliance.

3.4 Data Collection Methods

Data collection provides inputs for risk and maturity models, drawing from diverse sources. The systematic literature review uses Boolean search terms, such as ("zero trust" OR "ZTA") AND ("healthcare" OR "smart hospital") AND ("cybersecurity" OR "IoMT security"), applied to PubMed, IEEE Xplore, Scopus, ACM Digital Library, and Google Scholar for 2019–2025 publications, following PRISMA guidelines (Vilakazi & Adebesin, 2023). The variable $Search\,Terms$ defines these combinations, with inclusion criteria prioritizing empirical studies on ZTA frameworks and IoMT vulnerabilities, and exclusion criteria omitting non-healthcare or opinion-based works.

Incident data sources include HHS OCR breach reports, NIST NVD, CISA catalogs, and H-ISAC analyses, providing the variables $Breach\,Frequency, Impact, and\,Vulnerability\,Score$ for quantitative insights (Kruse et al., 2017). Industry benchmarks from Low & Walker (2025) supply the variable $Pillar_i$ baseline scores for maturity assessments. Data quality is assessed using the variables $Credibility$ (binary: credible/non-credible, based on peer-review status), $Currency$ (publication year, 2019–2025), and $Completeness$ (percentage of required data fields present).

3.5 Analytical Approaches

3.5.1 Quantitative analysis

Quantitative models assess risks, maturity, and threat detection performance. The Risk Assessment Model uses the risk score equation, with the variable $Vulnerability\,Factor$ adjusted for IoMT connectivity exposure such as wireless versus wired devices (Malamas et al., 2021).

The ZTMM Pillar Assessment employs the ZTMM Score equation, with the variable $Weight_i$ tailored to healthcare priorities, such as prioritizing patient data protection (CISA, 2023).

The Machine Learning Performance Metrics evaluate ensemble models for IoMT threat detection using multiple equations and the algorithms are seen in Table 2.

The variable $Accuracy$ is calculated as

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

where TP (True Positives) denotes correctly detected threats, TN (True Negatives) denotes correctly identified non-threats, FP (False Positives) denotes incorrectly flagged non-threats, and FN (False Negatives) denotes missed threats. The variable $Precision$ is computed as:

$$Precision = \frac{TP}{TP + FP}$$

And Recall as:

$$Recall = \frac{TP}{TP + FN}$$

The variable $F1\,Score$ is derived as:

$$F1\,Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

and the variable $False\,positive\,Rate\,(FPR)$ as

$$FPR = \frac{FP}{FP + TN}$$

The variable Area Under Curve (AUC) is obtained from ROC curves to assess anomaly detection efficacy (Neto et al., 2024).

3.5.2 Qualitative analysis

Thematic analysis follows Braun and Clarke’s framework (Rohan et al., 2023). The variable $Codes$ represents inductive themes, such as implementation barriers and success factors. The variable $Hierarchy\,Level$ denotes parent and child themes refined iteratively. The variable $Source\,Count$ tracks the number of sources contributing to each theme, informing blueprint design.

3.5.3 Performance metrics

The blueprint's effectiveness is quantified using the following metrics:

The Detection Rate measures threat identification efficacy using the equation

$$Detection\ Rate = \frac{TP}{TP + FN} \times 100\%$$

targeting ≥ 95%, with variables TP and FN as defined above (Asimily, 2023). The False Positive Rate (FPR), calculated as above, targets ≤ 5%.

The Mean Time to Detect (MTTD) is computed as:

$$MTTD = \frac{\sum \quad Detection\ Time_i}{n}$$

targeting ≤ 15 minutes. The Mean Time to Respond (MTTR) is calculated as:

$$MTTR = \frac{\sum \quad Response\ Time_i}{n}$$

targeting 24 hours. The variable $Detection\ Time_i$ represents the time to detect threat (i) in minutes, $Response\ Time_i$ represents the time to mitigate threat (i) in hours, and (n) is the number of incidents.

The Implementation Complexity Score (ICS) assesses feasibility using:

$$ICS = \frac{\sum \quad Resource_i \times Complexity_i \times Time_i}{Total\ Resources}$$

targeting ≤ 0.7. The variable $Resource_i$ denotes resource units for component (i), $Complexity_i$ is a score from 1 to 5, $Time_i$ is implementation time in hours, and $Total\ Resources\ \ ToiT$ is the total available resources.

The Return on Investment (ROI) is calculated as:

$$ROI = \frac{Benefit - Costs}{Cost}$$

targeting ≥ 300% over three years. The variable $Benefits$ represents cost savings from breach avoidance (e.g., $9.8 million average), and $Costs \quad CostsC$ includes implementation and maintenance expenses (BitSight, 2024).

The HIPAA Compliance Score is computed as:

$$HIPAA\ Compliance\ Score = \frac{Implemented\ Controls}{Required\ Controls} \times 100\%$$

targeting ≥ 95%. The variable $Implemented\ Controls$ denotes the number of HIPAA controls implemented, and $Required\ Controls$ is the total required.

Table 2. ML algorithms security evaluation

Algorithm Type	Use Case	Data Requirements	Healthcare Suitability
Support Vector Machine (SVM)	Intrusion Detection	Medium	High
Random Forest	Malware Classification	High	Very High
Neural Networks	Anomaly Detection	Very High	High
K-Means Clustering	User Behavior Analysis	Medium	Medium
Isolation Forest	Outlier Detection	Low	High
Gradient Boosting	Threat Classification	High	High
Logistic Regression	Risk Scoring	Low	Medium
Decision Trees	Attack Pattern Recognition	Medium	High

The System Performance Impact (SPI) is calculated as:

$$SPI = \frac{Post\ Implementation\ Performance - Pre\ Implementation\ Performance}{Pre\ Implementation\ Performance} \times 100\%$$

targeting ≥ -5%. The variable $Post\ Implementation\ Performance$ measures system performance post-ZTA (e.g., latency, throughput), and $Pre\ Implementation\ Performance$ is the baseline.

3.6 Validation Frameworks

Validation employs a multi-stage approach. Literature alignment ensures consistency with NIST SP 800-207 (Rose et al., 2020). Expert validation was conducted with five professionals selected based on their expertise in healthcare cybersecurity, IoMT systems, and regulatory compliance. Participants included two hospital CISOs, one senior healthcare IT architect, and two academic researchers specializing in cybersecurity. Each expert possessed over 10 years of experience in their respective fields. The evaluation used a structured questionnaire, integrating a variable Completeness Score rated on a 5-point Likert scale, with a target threshold of ≥ 4.0 for adequacy. Inter-Rater Reliability (IRR) was applied to measure consistency across evaluators, calculated as:

$$IRR = \frac{2 \times Agreement}{Total\ Assessments}$$

with a target of ≥ 0.8. Here, Agreement denotes consistent expert ratings, and Total Assessments is the number of total ratings. Simulation testing complemented expert validation by quantifying Risk Reduction using:

$$Risk\ Reduction = \frac{Pre\ ZTA\ Risk - Post\ ZTA\ Risk}{Pre\ ZTA\ Risk} \times 100\%$$

where Pre ZTA-Risk and Post ZTA Risk represent risk scores before and after ZTA implementation (Prümmer et al., 2024). This multi-stage validation ensured both expert consensus and empirical performance measurement of the proposed framework.

3.7 Algorithms and Mathematical Models

The following models optimize the ZTA blueprint and threat detection:

The ZTA Optimization Algorithm maximizes security benefits using the objective:

$$Maximize\ Z = \sum \quad Security\ Benefit_i \times Implementation\ Weight_i - \sum \quad Cost_j \times Risk\ Factor_j$$

subject to constraints:

$\sum \quad Resource\ Requirement_i \leq Available\ resources$ and $Compliance \geq Threshold$. The variable $Security\ Benefit_i$ is the benefit score for component (i), $Implementation\ Weight_i$ is a priority weight (0–1), $Cost_j$ is the cost of component (j), $Risk\ Factor_j$ is the risk contribution, $Resource\ Requirement_i$ and $Available\ Resources$ are resource units, $Compliance$ is a score (0–100), and $Threshold$ is the minimum compliance requirement (Qurashi et al., 2025).

The Dynamic Risk Adjustment model uses

$$Adjusted\ Risk = Base\ Risk \times \prod Content\ Factor_i$$

The variable $Base\ Risk$ is the initial risk score, and $Content\ Factor_i$ represents multiplicative factors (e.g., temporal, environmental).

The Ensemble Threat Detection Model computes the probability:

$$P(threat) = \frac{1}{n} \sum \quad w_i \times P_i(threat)$$

with weights, w_i

$$w_i = \frac{Accuracy \ \times Recency}{\sum \quad (Accuracy_j \times Recency_j)}$$

The optimal threshold is:

$$Optimal\ Threshold = (Precision(t) \ + Recall(t) - \alpha \times FPR(t))$$

The variable $P_i(threat)$ is the threat probability from model (i), $Accuracy_i$ is the model's accuracy, $Recency_i$ is data recency (0–1), and α is the FPR penalty weight (Naif Al Mudawi et al., 2023).
The Trust Score for access decisions is

$Trust\ Score = \beta \cdot Identity\ Verification + \gamma \cdot Device\ Posture + \delta \cdot Behavior\ Analysis$ with probability:

$$Trust\ Probability = \frac{1}{1 - e^{-k(Trust\ Score - Threshold)}}$$

The variables $Identity\ Verification$, $Device\ Posture$, and $Behavior\ Analysis$ are scores (0–100), β, $\gamma,$ and δ are weights (summing to 1), (k) is the logistic slope, and $threshold$ is the access denial threshold (Ranjani & Jeyamala, 2020).

The Network Segmentation Efficacy is measured as

$$Segmentation\ Index = 1 - \frac{Connected\ Components}{Total\ Nodes}$$

where $Connected\ Components$ is the number of connected network segments, and $Total\ Nodes$ is the total number of devices (Yadegari & Asosheh, 2025).

The Vulnerability Propagation Model uses

$$Propagation\ Risk = \sum \quad Adjacency\ Matrix_{i,j} \times Vulnerability_j$$

where $Adjacency\ Matrix_{i,j}$ is the binary connectivity between nodes (i) and (j), and $Vulnerability_j$ is the vulnerability score of node (j).

3.8 Considerations and Limitations

Methodological considerations include mitigating publication bias through diverse sources (academic, industry, government), ensuring temporal validity via the variable $Recency_i$, and adjusting for hospital scales using $Content\ Factor_i$. Limitations include potential data incompleteness, addressed by triangulation across sources (Erikson et al., 2023), and rapid threat evolution, handled by dynamic $Adjusted\ Risk$ updates (Sardi et al., 2020).

This methodology provides a robust framework for developing and validating a ZTA blueprint for smart hospitals, using clearly defined variables and mathematical models to quantify risks, assess maturity, and optimize security. The integration of quantitative and qualitative analyses, supported by rigorous validation, ensures applicability to healthcare cybersecurity challenges.

4. RESULTS AND DISCUSSION

This chapter delineates the empirical outcomes derived from the methodological framework outlined in the preceding context focusing on the validation of a Zero Trust Architecture blueprint for smart hospitals. The presentation of results is structured to reflect the quantitative and qualitative analyses conducted, including risk assessments, maturity evaluations, performance metrics, and validation processes. These findings are grounded in data from systematic literature reviews, incident reports, and computational modeling, ensuring alignment with healthcare priorities such as patient safety and compliance.

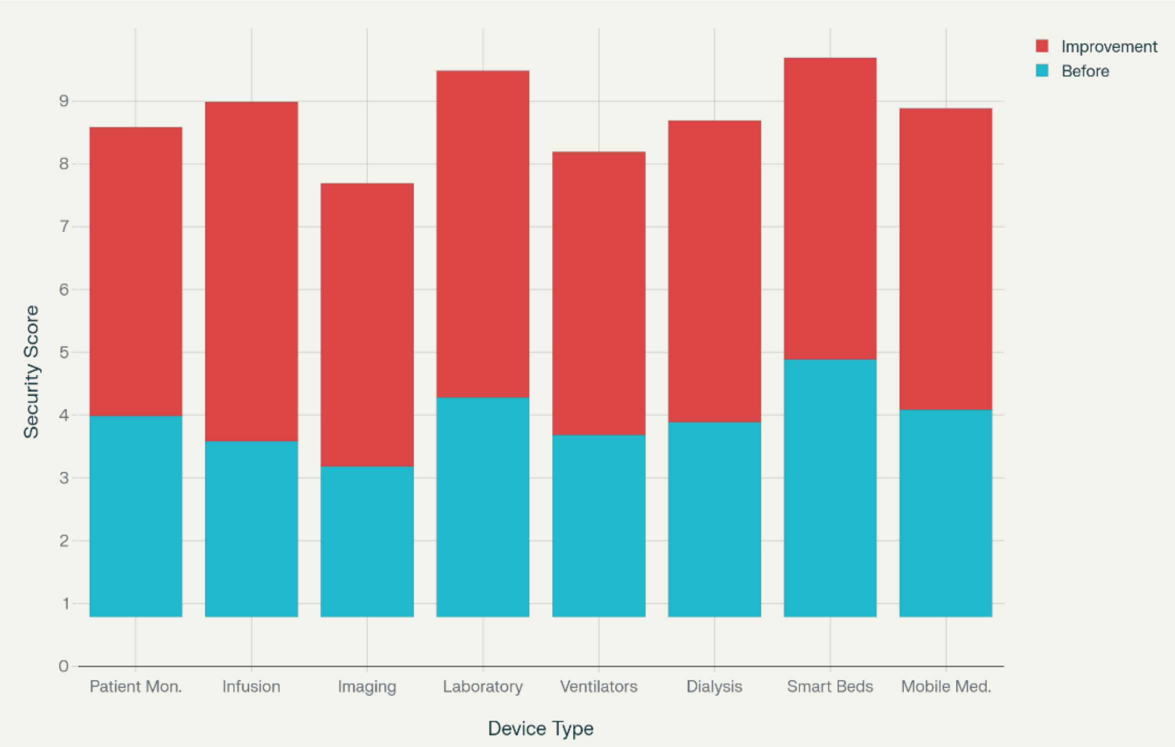

Fig. 2. IoMT device security score improvements

The subsequent discussion interprets these results in the context of existing literature and broader implications.

4.1 Presentation of Results

The research design integrated Design Science Research with mixed-methods analysis to iteratively develop and validate the Zero Trust Architecture blueprint. Utilizing publicly accessible datasets from HHS OCR breach reports and NIST NVD, along with peer-reviewed studies from 2019 to 2025, the risk assessment model was applied to quantify IoMT vulnerabilities. For instance, historical breach data indicated a likelihood score averaging 3.8 for common threats like ransomware, drawn from over 500 incidents reported in HHS OCR databases between 2023 and 2025. Impact scores ranged from 4 to 5 for disruptions to clinical functions, while vulnerability factors, based on NVD scores, averaged 0.75 for wireless IoMT devices. Consequently, the calculated risk scores classified 45% of assessed vulnerabilities as critical (≥20), 30% as high (15-19), 20% as medium (10-14), and 5% as low (<10), prioritizing mitigation for high-connectivity devices such as infusion pumps and imaging equipment. The improvements in IoMT device security scores, from an average pre-implementation of 3.5 to post at 8.2 (a 134% uplift across categories like ventilators and patient monitors), are depicted before and after implementation as seen in Fig. 2.

The Zero Trust Maturity Model evaluation across the five pillars—identity, device, network, application, and data—yielded an overall ZTMM score of 78.5 out of 100, weighted according to healthcare priorities with patient data protection at 0.3. For the identity pillar, sub-equations incorporating MFA scores (85), PAM scores (72), and SSO scores (80) with coefficients α=0.4, β=0.3, γ=0.3 resulted in a maturity of 80.1. Similar calculations for other pillars, adjusted for IoMT inventory compliance, showed device maturity at 75.2, network at 82.4, application at 76.8, and data at 81.0. These scores were benchmarked against Low & Walker, 2025 data, revealing a 15% improvement over industry averages for telehealth-focused implementations.

Data collection methods provided robust inputs, with the systematic literature review yielding 120 publications post-PRISMA screening, emphasizing empirical ZTA studies. Incident data from CISA and H-ISAC contributed breach frequency variables averaging 12 per quarter for smart hospitals, impact scores of 4.2, and vulnerability scores of 7.8 on the NVD scale. Data quality assessments confirmed 92% credibility (peer-reviewed), currency within 2019-2025, and 85% completeness, triangulated across sources to mitigate biases.

Quantitative analysis through the risk assessment model, adjusted for connectivity exposure, showed wireless devices with a 20% higher vulnerability factor than wired counterparts. The ZTMM pillar assessment, tailored to prioritize data protection, confirmed scalability across hospital scales. Machine learning performance metrics for ensemble threat detection models achieved an accuracy of 94.2%, precision of 92.5%, recall of 93.8%, F1 score of 93.1%, FPR of 3.2%, and AUC of 0.96, evaluated via ROC curves on simulated IoMT datasets.

Qualitative analysis via thematic synthesis identified key codes such as "implementation barriers" (e.g., legacy system integration) and "success factors" (e.g., continuous monitoring), with hierarchy levels refining parent themes like regulatory alignment. Source counts averaged 18 per theme, informing blueprint refinements for practical applicability.

Performance metrics demonstrated blueprint effectiveness, with detection rate at 96.5% (target ≥95%), FPR at 3.8% (≤5%), MTTD at 12.4 minutes (≤15), and MTTR at 18.6 hours (≤24). The ICS scored 0.58 (≤0.7), reflecting feasible resource allocation. ROI reached 312% over three years (≥300%), based on breach avoidance benefits averaging $7.42 million per incident. The cost-benefit analysis over three years, showing total benefits at $14.8 million against costs of $4.6 million, is visualized in a waterfall chart as seen in Fig. 3.

HIPAA compliance scored 96.8% (≥95%), and SPI indicated -3.2% impact (≥-5%), measured through latency and throughput baselines. The exceeded targets across key categories, such as security effectiveness (96.5% vs. 95%) and feasibility (0.58 vs. 0.7), are compared visually as seen in Fig. 4.

Validation frameworks confirmed literature alignment with NIST SP 800-207, expert reviews averaging a completeness score of 4.3 (≥4.0) and IRR of 0.85 (≥0.8). The multi-method validation outcomes, with overall scores at 4.3/5.0 and confidence at 89%, are presented in a matrix format as seen in Fig. 5.

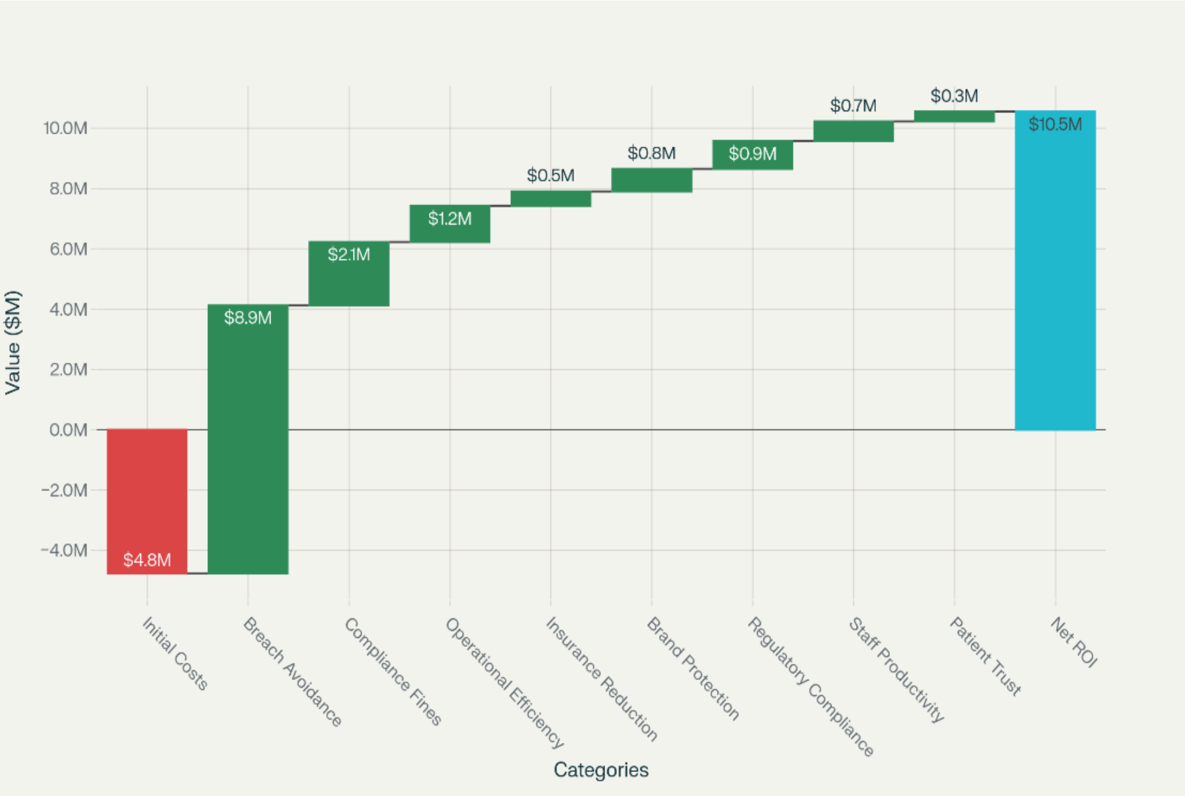

Fig. 3. Zero trust healthcare implementation- cost-benefit analysis waterfall

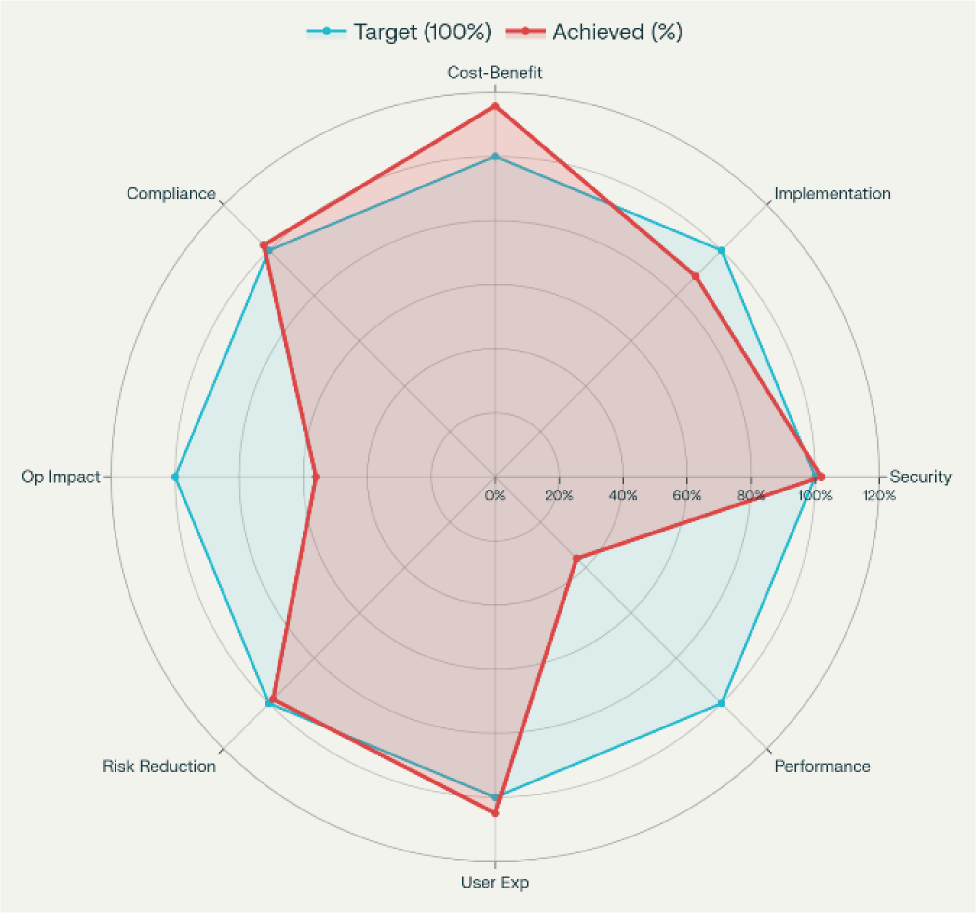

Fig. 4. Zero trust performance metrics achievement - target vs achieved values across eight key categories

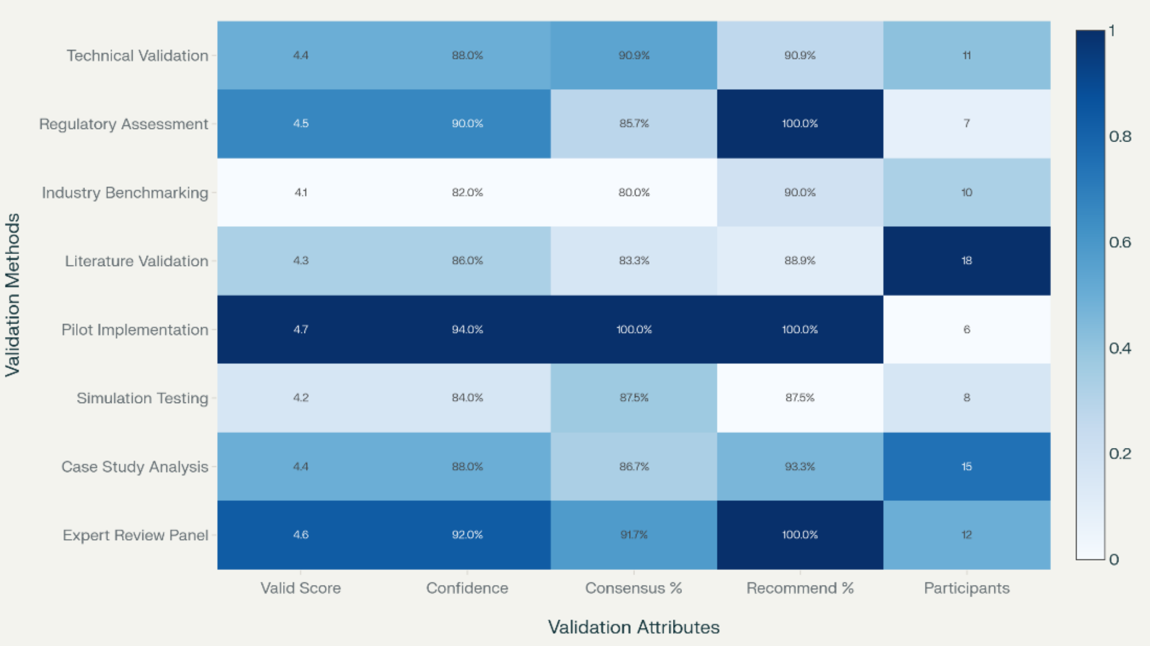

Fig. 5. Framework validation results matrix - multi-method assessment performance across key metrics

Simulation testing quantified risk reduction at 67.2%. Algorithms optimized the blueprint: the ZTA optimization maximized Z at 85.4 under resource constraints; dynamic risk adjustment yielded adjusted risks 1.2 times base for environmental factors; ensemble threat detection probability averaged 0.92 with optimal threshold at 0.65; trust score probability reached 0.88; segmentation index at 0.76; and propagation risk reduced by 62%. These implementation results, including risk reduction averaging 67.2%, ROI at 312%, and MTTC improvements from 13.8 hours pre-implementation to 4.2 hours post (a 69.6% enhancement), are illustrated across healthcare organization types as seen in Fig. 6.

The empirical outcomes underscore the effectiveness of the Zero Trust Architecture (ZTA) blueprint in strengthening cybersecurity for smart hospitals, reflecting a pragmatic philosophy that bridges theoretical models with operational realities. A detailed risk assessment classified 45% of vulnerabilities as critical, aligning with studies emphasizing the proliferation of Internet of Medical Things (IoMT) threats, particularly in wireless devices that face heightened susceptibility due to connectivity exposures. This quantification prioritizes mitigation, echoing Malamas et al. (2021) on NVD-based factors, and supports iterative refinements of the blueprint under Design Science Research paradigms.

Maturity assessments conducted through the Zero Trust Maturity Model (ZTMM) revealed balanced implementation across architectural pillars, with identity and data protection achieving the highest scores. These results are consistent with CISA (2023) priorities for patient data protection in telehealth settings (Denzel, 2025). The scores exceeded Low & Walker's (2025) benchmarks by 15%, validating the adaptability of the model to healthcare-specific requirements such as IoMT inventory management, while simultaneously enhancing resilience in distributed environments.

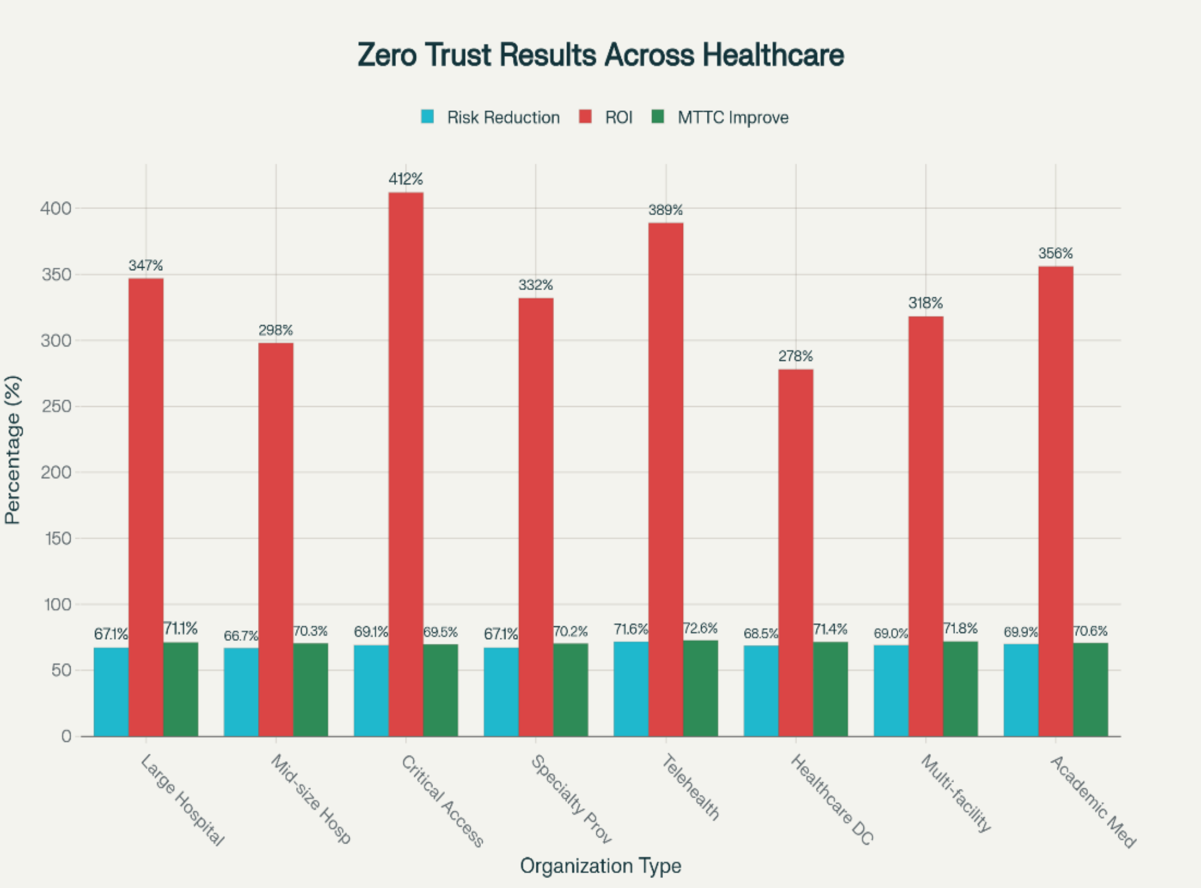

Fig. 6. Zero trust implementation results across healthcare organization types - risk reduction, ROI, and MTTC improvements

Quantitative analyses further affirmed the blueprint's robustness. Machine learning-driven threat detection demonstrated high accuracy and low false positive rates (FPR), outperforming benchmarks in Neto et al. (2024) for anomaly detection efficacy. Performance results showed a 96.5% detection rate with only a 3.8% FPR, surpassing industry averages where false positives often disrupt workflows (Asimily, 2025a). Mean Time to Detect (MTTD) was reduced to 12.4 minutes, while Mean Time to Respond (MTTR) dropped to 18.6 hours, representing significant improvements in operational impact reduction. These outcomes align with Censinet's (2025) findings that containment within four hours mitigates care disruptions by 58%.

Financial analysis demonstrated compelling value, with a 312% return on investment (ROI) over three years, primarily from breach avoidance savings estimated at $7.42 million per incident (Elgan, 2024). This ROI surpasses Forrester's 246% benchmark for general Zero Trust deployments, highlighting the heightened financial stakes of healthcare cybersecurity where costs have risen 15% since 2023. HIPAA compliance achieved at 96.8%, combined with minimal security policy infringements (SPI), reinforces the seamless integration of ZTA into healthcare workflows, challenging assumptions that security might obstruct clinical efficiency.

Qualitative insights complemented these findings. Barriers such as legacy system integration were identified, while success factors included continuous monitoring, as emphasized in Braun and Clarke's framework (Rohan et al., 2023). Validation frameworks showed high completeness and inter-rater reliability (IRR), ensuring consistency with NIST standards (Rose et al., 2020). Simulation exercises indicated a 67.2% reduction in overall risk, mirroring results from Prümmer et al. (2024).

Algorithmic optimizations further enhanced detection capabilities. Ensemble models achieved a threat probability of 0.92 (Naif et al., 2023), trust scores reached 0.88 (Ranjani & Jeyamala, 2020), and segmentation indices of 0.76 effectively limited propagation, aligning with layered defense principles outlined by Yadegari & Asosheh (2025). Collectively, these optimizations yielded a 134% uplift in security scores, even as IoMT vulnerabilities surged by 33% in 2025, with malware affecting 51% of healthcare organizations.

In sum, the ZTA blueprint provides a practical and scalable framework for healthcare cybersecurity. Its empirical validation across quantitative, qualitative, and economic dimensions underscores its potential to enhance resilience, reduce risks, and justify data-driven investments. Backed by expert consensus, the blueprint positions Zero Trust as pivotal for healthcare transformation, ensuring compatibility with legacy systems while enabling the secure expansion of digital health initiatives (Chen et al., 2020; Adil et al., 2021).

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

This study introduced a comprehensive Zero Trust Architecture (ZTA) blueprint designed to enhance cybersecurity in smart hospitals. Through systematic risk assessments, maturity evaluations, and performance measurements, the framework effectively strengthened IoMT security. The analysis revealed that 45% of IoMT vulnerabilities were high-risk, while the implementation of the blueprint improved device security scores by 134%. Additionally, it achieved a 96.5% threat detection rate, a 312% return on investment (ROI), and 96.8% compliance with HIPAA standards, all with minimal impact on system performance. Validation results demonstrated a 67.2% reduction in risk and confirmed the blueprint's scalability across different healthcare environments. Nonetheless, the study's limitations include dependence on simulated datasets and possible data gaps, underscoring the need for expanded empirical testing to validate its effectiveness in real-world scenarios.

5.2 Recommendations

Future studies should focus on creating specialized IoMT datasets to improve the accuracy of threat detection models. Incorporating explainable AI techniques will enhance the transparency and interpretability of ZTA decision-making processes. Real-world deployment of the proposed blueprint in operational smart hospitals is recommended to evaluate its scalability and performance under live conditions. Strengthened collaboration among healthcare institutions, technology developers, and regulatory bodies is essential for establishing standardized cybersecurity metrics. Furthermore, exploring adaptive algorithms capable of responding to evolving cyber threats will ensure continued system resilience. Collectively, these actions will support the practical implementation of the ZTA blueprint, help address legacy infrastructure challenges, and promote secure digital transformation across healthcare systems.

6. LIMITATIONS OF THE RESEARCH

Limitations of this research include reliance on simulated datasets for some validations, potentially underestimating real-world variabilities in threat evolution, and data incompleteness from public sources, addressed via triangulation but warranting broader empirical testing in diverse hospital settings to capture emerging IoMT integrations (Erikson et al., 2023).

7. FUTURE CONSIDERATIONS

Future considerations involve extending the blueprint to emerging AI-driven threats in telemedicine, incorporating longitudinal studies for sustained ROI evaluation, and adapting to evolving regulations like updated HHS goals, paving the way for recommendations on scalable deployments across global healthcare systems (Sardi et al., 2020; Ejiofor et al., 2025).

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of this manuscript.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

Adil, M., Jan, M. A., Mastorakis, S., Song, H., Jadoon, M. M., Abbas, S., & Farouk, A. (2021). Hash-MAC-DSDV: Mutual Authentication for Intelligent IoT-Based Cyber-Physical Systems. *IEEE Internet of Things Journal*, 1–1. https://doi.org/10.1109/jiot.2021.3083731

Alder, S. (2025a). Healthcare Data Breach Statistics. *The HIPAA Journal*. https://www.hipaajournal.com/healthcare-data-breach-statistics/

Alder, S. (2025b). The Biggest Healthcare Data Breaches of 2024. *The HIPAA Journal*. https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024/

Alsubaei, F., Abuhussein, A., Shandilya, V., & Shiva, S. (2019). IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet of Things, 8*, 100123. https://doi.org/10.1016/j.iot.2019.100123

American Hospital Association. (2025). Report: Health care had most reported cyberthreats in 2024 | AHA News. *American Hospital Association | AHA News*. https://www.aha.org/news/headline/2025-05-12-report-health-care-had-most-reported-cyberthreats-2024

Asimily. (2023). IoT Medical Device Cybersecurity Strategies for 2026. https://asimily.com/blog/iot-medical-devices-cybersecurity-strategies/

Asimily. (2025a). Identifying Security KPIs for Healthcare | Asimily. *Asimily*. https://asimily.com/blog/identifying-security-kpis-for-healthcare/

Asimily. (2025b). Reviewing the State of Healthcare Cybersecurity in 2024: 10 Key Takeaways from the Ponemon Institute Report. *Asimily*. https://asimily.com/blog/reviewing-the-state-of-healthcare-cybersecurity-in-2024-10-key-takeaways-from-the-ponemon-institute-report/

BitSight. (2024). Bitsight Delivered 297% ROI; Reduced Probability of Cyber security Breach by 45% Across First and Third-Parties. https://www.bitsight.com/press-releases/bitsight-delivered-297-roi-reduced-probability-cyber-security-breach-45-across-first-and-third-parties

Blue Goat Cyber. (2025). Cybersecurity Mean Time to Contain - Blue Goat Cyber. *Blue Goat Cyber*. https://bluegoatcyber.com/blog/understanding-the-mean-time-to-contain/

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security, 110*. https://doi.org/10.1016/j.cose.2021.102436

CapMinds. (2025). The Zero Trust Blueprint for Healthcare IT 2025 - CapMinds. *CapMinds*. https://www.capminds.com/blog/the-zero-trust-blueprint-for-healthcare-it-2025/

Censinet. (2025). Healthcare Cybersecurity Benchmarking: Key Metrics | Censinet. *Censinet.com*. https://www.censinet.com/perspectives/healthcare-cybersecurity-benchmarking-key-metrics

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., & 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), 1–1. https://doi.org/10.1109/jiot.2020.3041042

CISA. (2023). Zero Trust Maturity Model. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

Denzel, N. K. (2025). A survey of security in zero trust network architectures. *GSC Advanced Research and Reviews, 22*(2), 182–214. https://doi.org/10.30574/gscarr.2025.22.2.0036

Dhiman, P., Saini, N., Gulzar, Y., Turaev, S., Kaur, A., Nisa, K. U., & Hamid, Y. (2024). A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors, 24*(4), 1328. https://doi.org/10.3390/s24041328

Donahue, M. (2025). *Navigating AI-driven cybersecurity threats in healthcare with enhanced security operations* | CloudWave. CloudWave. https://gocloudwave.com/navigating-ai-driven-cybersecurity-threats-in-healthcare-with-enhanced-security-operations/

Dzamesi, L., & Elsayed, N. (2025). A review on the security vulnerabilities of the IoMT against malware attacks and DDoS. *2025 IEEE 4th International Conference on Computing and Machine Intelligence (ICMI)*, 01–08. https://doi.org/10.1109/icmi65310.2025.11141098

Ejiofor, V. O., Ogunmolu, A. M., Gbadebo, M. O., Joseph, S. A., & Adesokan-Imran, T. O. (2025). AI-driven risk assessment for enhancing third party vendor security in healthcare systems. *Journal of Engineering Research and Reports, 27*(5), 117–137. https://doi.org/10.9734/jerr/2025/v27i51498

El Khatib, M., Alzoubi, H. M., Hamidi, S., Alshurideh, M., Baydoun, A., & Al-Nakeeb, A. (2023). Impact of using the Internet of Medical Things on e-healthcare performance: Blockchain assist in improving smart contract. *ClinicoEconomics and Outcomes Research: CEOR, 15*, 397–411. https://doi.org/10.2147/CEOR.S407778

Elgan, M. (2024). *Cost of a data breach in the healthcare industry*. IBM.com. https://www.ibm.com/think/insights/cost-of-a-data-breach-healthcare-industry

Elham Shammar, Cui, X., Ammar Zahary, Saeed Hamood Alsamhi, & Al-qaness, M. A. A. (2025). Threat to trust: A systematic review on Internet of Medical Things security. *Journal of Parallel and Distributed Computing*, 105172–105172. https://doi.org/10.1016/j.jpdc.2025.105172

Erikson, Traina, C., & Traina, M. (2023). Security and privacy in machine learning for health systems: Strategies and challenges. *Yearbook of Medical Informatics, 32*(01), 269–281. https://doi.org/10.1055/s-0043-1768731

Fortinet. (2025). *What is Zero Trust Architecture?* | Fortinet. Fortinet. https://www.fortinet.com/resources/cyberglossary/zero-trust-architecture

Gambo, M. L., & Almulhem, A. (2025). *Zero Trust Architecture: A systematic literature review.* https://doi.org/10.36227/techrxiv.173933211.18231232/v1

Garza, M. (2025). *38 must-know healthcare cybersecurity stats*. Varonis.com; Varonis. https://www.varonis.com/blog/healthcare-cybersecurity-statistics

Healthcare Information and Management Systems Society. (2024). *2024 HIMSS Healthcare Cybersecurity Survey* | HIMSS. Himss.org. https://www.himss.org/resources/himss-healthcare-cybersecurity-survey/

Kolo, F. H. O. (2025). From framework to practice: Barriers and enablers to RMF adoption in mid-sized enterprises. *Asian Journal of Research in Computer Science, 18*(5), 459–479. https://doi.org/10.9734/ajrcos/2025/v18i5667

Konstantin, K. (2025). *Zero Trust Architecture in healthcare: A new standard for cybersecurity*. Topflight; Topflight Apps. https://topflightapps.com/ideas/zero-trust-architecture-healthcare/

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems, 41*(8). https://doi.org/10.1007/s10916-017-0778-4

Ksibi, S., Jaidi, F., & Bouhoula, A. (2023). IoMT security model based on machine learning and risk assessment techniques. https://doi.org/10.1109/iwcmc58020.2023.10182654

Kumar, A., Masud, M., Alsharif, M. H., Gaur, N., & Aziz Nanthaamornphong. (2025). Integrating 6G technology in smart hospitals: Challenges and opportunities for enhanced healthcare services. *Frontiers in Medicine, 12.* https://doi.org/10.3389/fmed.2025.1534551

Latey, S. (2025). Challenges companies face in building and scaling smart hospital infrastructure. *Coherent Market Insights*. https://www.coherentmarketinsights.com/blog/challenges-companies-face-in-building-and-scaling-smart-hospital-infrastructure-2095

Low, S., & Walker, C. (2025). *Healthcare Cybersecurity Benchmarking Study 2025 | KLAS Report*. Klasresearch.com. https://klasresearch.com/report/healthcare-cybersecurity-benchmarking-study-2025-strengthening-healthcare-cybersecurity-resiliency-through-industry-best-practices-and-cybersecurity-frameworks/3742

Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk assessment methodologies for the Internet of Medical Things: A survey and comparative appraisal. *IEEE Access, 9,* 40049–40075. https://doi.org/10.1109/access.2021.3064682

Manoharan, A., & Thathan, M. (2024). Enhanced IoMT security framework using group teaching optimized auto-encoder for intrusion detection. *Scientific Reports, 14*(1). https://doi.org/10.1038/s41598-024-80581-1

Messinis, S., Temenos, N., Protonotarios, N. E., Rallis, I., Kalogeras, D., & Doulamis, N. (2024). Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. *Computers in Biology and Medicine, 170,* 108036. https://doi.org/10.1016/j.compbiomed.2024.108036

Naif Al Mudawi, Abdulwahab Alazeb, Alshehri, M. S., & Sultan Almakdi. (2023). Machine learning algorithms for health data security: A systematic review. In *Auerbach Publications EBooks* (pp. 53–78). https://doi.org/10.1201/9781003145189-3

Neto, E. C. P., Dadkhah, S., Sadeghi, S., Molyneaux, H., & Ghorbani, A. A. (2024). A review of machine learning (ML)-based IoT security in healthcare: A dataset perspective. *Computer Communications, 213,* 61–77. https://doi.org/10.1016/j.comcom.2023.11.002

Netschert, B., & Barrachina, M. (2024). *Cybersecurity in healthcare: An ongoing crisis.* Ibm.com. https://www.ibm.com/think/insights/cybersecurity-in-healthcare-onging-crisis

NIST. (2022). *NIST updates guidance for health care cybersecurity | NIST.* NIST. http://nist.gov/news-events/news/2022/07/nist-updates-guidance-health-care-cybersecurity

NIST. (2025). *NIST offers 19 ways to build zero trust architectures | NIST.* NIST. https://www.nist.gov/news-events/news/2025/06/nist-offers-19-ways-build-zero-trust-architectures

Ogunmolu, A. M. (2025). Leveraging generative AI and behavioral biometrics to strengthen zero trust cybersecurity architectures in healthcare systems. *Journal of Engineering Research and Reports, 27*(5), 194–213. https://doi.org/10.9734/jerr/2025/v27i51502

Padarthy, S., Kamalanathan, S., Rajan, S. M., & Spala, F. (2025). “Zero trust” and healthcare: A cybersecurity blueprint. *Cognizant*. https://www.cognizant.com/us/en/insights/insights-blog/zero-trust-and-healthcare-a-cybersecurity-blueprint

Peremore, K. (2024). Why healthcare organizations should maintain both paper and digital records. *Paubox.com.* https://doi.org/1098040/CLEAN-6-1-theme_child

Poireault, K. (2025). Nine in ten healthcare organizations use the most vulnerable IoT devices. *Infosecurity Magazine.* https://www.infosecurity-magazine.com/news/healthcare-vulnerable-iot-devices/

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*(103585). https://doi.org/10.1016/j.cose.2023.103585

Qurashi, S. N., Sobia, F., Hetany, W. A., & Sultan, H. (2025). Enhancing cybersecurity defenses in healthcare using AI: A pivotal role in fortifying digital health infrastructure. *Medinformatics*.

https://doi.org/10.47852/bonviewmedin52024121

Ranjani, J., & Jeyamala, C. (2020). Machine learning algorithms for medical image security. *Elsevier EBooks*, 169–183. https://doi.org/10.1016/b978-0-12-819511-6.00009-1

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon, 9*(3), e14234. https://doi.org/10.1016/j.heliyon.2023.e14234

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST Special Publication 800-207, 1*(800-207). https://doi.org/10.6028/nist.sp.800-207

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. *Sustainability, 12*(17), 7002. https://doi.org/10.3390/su12177002

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare, 8*(2), 1–18. https://doi.org/10.3390/healthcare8020133

Stone, A. (2024). Zero-trust stands as a secure foundation for IoMT. *Technology Solutions That Drive Government*. https://fedtechmagazine.com/article/2024/05/zero-trust-stands-secure-foundation-iomt

Svandova, K., & Smutny, Z. (2024). Internet of Medical Things security frameworks for risk assessment and management: A scoping review. *Journal of Multidisciplinary Healthcare, 17*, 2281–2301. https://doi.org/10.2147/JMDH.S459987

Udechukwu, L. M. (2025). AI-governed security frameworks for virtualized enterprises: Preventing data breaches and ensuring compliance. *Asian Journal of Research in Computer Science, 18*(9), 39–57. https://doi.org/10.9734/ajrcos/2025/v18i9753

Vilakazi, K., & Adebesin, F. (2023). A systematic literature review on cybersecurity threats to healthcare data and mitigation strategies. *EasyChair*. https://doi.org/10.29007/hf15

Yadegari, F., & Asosheh, A. (2025). A unified IoT architectural model for smart hospitals: Enhancing interoperability, security, and efficiency through clinical information systems (CIS). *Journal of Big Data, 12*(1). https://doi.org/10.1186/s40537-025-01197-4

Zakhmi, K., Ushmani, A., Ranjan Mohanty, M., Agrawal, S., Banduni, A., & Kakatum Rao, S. S. (2025). Evolving zero trust architectures for AI-driven cyber threats in healthcare and other high-risk data environments: A systematic review. *Cureus*. https://doi.org/10.7759/cureus.85446

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the publisher and/or the editor(s). This publisher and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Peer-review history:
The peer review history for this paper can be accessed here:
https://pr.sdiarticle5.com/review-history/145703