© NOV 2022 | IRE Journals | Volume 6 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV6I5-1712991

AI-Driven Supply Chain Security Framework for Healthcare IoT Ecosystems: A Zero-Trust Approach to Medical Device Vulnerability Management

OMOWUNMI FOLASHAYO MAKINDE[1], NATHANIEL ADENIYI AKANDE[2], ADETUNJI OLUDELE ADEBAYO[3], SOPULUCHUKWU ANI[4], OLATUNDE AYOMIDE OLASEHAN[5]
[1]*Amazon, USA*
[2]*Department of Computer Science, University of Bradford, UK*
[3]*First Bank of Nigeria, Plc*
[4]*Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria*
[5]*Department of Computer Science, Swansea University, UK*

Abstract- The proliferation of Internet of Things (IoT) devices in healthcare environments has fundamentally transformed patient care delivery while simultaneously introducing significant cybersecurity vulnerabilities throughout medical device supply chains. This research proposes an integrated security framework combining artificial intelligence capabilities with Zero Trust architecture principles to address critical vulnerabilities affecting medical devices from manufacturing through deployment and ongoing operations. Through comprehensive analysis of supply chain weaknesses, AI-driven detection techniques, and Zero Trust controls, this study demonstrates how these complementary approaches create defense-in-depth protecting against firmware manipulation, counterfeit components, distribution vulnerabilities, and inconsistent update mechanisms. The framework provides healthcare organizations with actionable guidance for implementing continuous monitoring, device authentication, behavioral analytics, and policy enforcement while accommodating clinical operational requirements. Recommendations address stakeholder responsibilities across hospitals, device manufacturers, and regulatory bodies to strengthen medical device security posture comprehensively.

Keywords: Healthcare IoT, Medical Device Security, Supply Chain Vulnerability, Zero Trust Architecture, Artificial Intelligence, Cybersecurity Framework, Firmware Integrity, Device Authentication

I. INTRODUCTION

1.1 Background

The healthcare sector has experienced unprecedented adoption of Internet of Things technologies, with connected medical devices becoming integral to modern patient care delivery. From insulin pumps and cardiac monitors to infusion systems and diagnostic equipment, IoT-enabled devices generate continuous patient data streams that enhance clinical decision-making while enabling remote monitoring and automated treatment adjustments. This rapid expansion of healthcare IoT ecosystems has introduced complex cybersecurity challenges that extend beyond traditional network security boundaries. Medical devices often operate with legacy operating systems, unpatched software, and limited built-in security capabilities. Many devices lack encryption for data transmission, employ weak or default authentication credentials, and provide no mechanisms for security updates. The mission-critical nature of healthcare operations compounds these technical vulnerabilities, as devices cannot be taken offline for security assessments without potentially disrupting patient care (Ghubaish et al., 2021).

Supply chain security has emerged as a critical concern within healthcare IoT ecosystems. Medical devices traverse complex global supply chains involving multiple manufacturers, distributors, integrators, and service providers before reaching clinical environments. Each supply chain stage introduces potential vulnerability points where adversaries can compromise device integrity, inject malicious code, or substitute counterfeit components. Traditional security controls focusing on perimeter defense and endpoint protection prove insufficient against sophisticated supply chain attacks that compromise devices before deployment (Thomasian & Adashi, 2021).

1.2 Problem Statement

Traditional security approaches in healthcare environments rely on perimeter-based defenses that assume internal network traffic can be trusted once authentication occurs. This paradigm fails to address supply chain vulnerabilities where medical devices arrive at healthcare facilities already compromised through firmware manipulation, counterfeit components, or unauthorized modifications during distribution (Baker, 2022). The distributed nature of medical device supply chains creates multiple attack surfaces that adversaries exploit to introduce vulnerabilities bypassing perimeter security controls.

Healthcare organizations struggle to maintain comprehensive visibility into device provenance, component authenticity, and firmware integrity throughout the supply chain lifecycle. Existing security controls often lack capabilities for continuous device identity verification, behavioral monitoring to detect compromised devices, or cryptographic validation of firmware updates. The absence of these capabilities leaves healthcare organizations vulnerable to advanced persistent threats that exploit supply chain weaknesses to establish persistent presence within clinical networks (Ghubaish et al., 2021).

The challenge is compounded by regulatory complexity and the mission-critical nature of healthcare operations. Medical devices cannot be taken offline for extended security assessments without disrupting patient care. Manufacturers prioritize device availability and clinical functionality over security hardening. Healthcare IT staff lack specialized expertise and resources necessary for comprehensive medical device security management (Ghubaish et al., 2021). These constraints necessitate security frameworks that provide robust protection while accommodating clinical operational requirements.

1.3 Purpose of the Study

This research investigates how artificial intelligence capabilities and Zero Trust security principles can be integrated to strengthen supply chain visibility and vulnerability management for medical devices throughout their operational lifecycles. The study examines specific AI techniques including behavioral profiling, anomaly detection, firmware integrity analysis, and predictive risk scoring that address supply chain vulnerabilities (Radanliev & De Roure, 2022). Concurrently, the research analyzes Zero Trust controls including continuous device authentication, network segmentation, verified firmware updates, and comprehensive audit logging that enforce security policies throughout the device lifecycle. The research aims to develop a comprehensive framework that addresses supply chain vulnerabilities from manufacturing through deployment and ongoing operations. This framework provides healthcare organizations with actionable guidance for implementing AI-enhanced monitoring and Zero Trust verification while maintaining clinical operational requirements. The integrated approach demonstrates how complementary technologies create defense-in-depth exceeding capabilities of individual security measures implemented in isolation (Markus et al., 2021).

1.4 Significance of the Study

This research contributes to healthcare cybersecurity by addressing critical gaps in medical device supply chain security. The integrated framework enhances patient safety by reducing the likelihood of device compromises that could directly harm patients through unauthorized device manipulation or indirect harm through data breaches exposing sensitive health information. By providing continuous monitoring and authentication capabilities, the framework enables healthcare organizations to detect and respond to threats before they impact clinical operations (He et al., 2021).

The study supports regulatory compliance by aligning with guidance from the Food and Drug Administration (FDA), National Institute of Standards and Technology (NIST), and other regulatory bodies emphasizing medical device cybersecurity throughout product lifecycles. The framework provides structured approaches for implementing regulatory requirements while accommodating diverse organizational capabilities and resource constraints (Smith et al., 2022).

From a broader perspective, this research advances the field of healthcare IoT security by demonstrating how emerging technologies can address long-standing vulnerabilities. The integration of AI and Zero Trust principles establishes a model applicable beyond medical devices to other critical infrastructure sectors facing similar supply chain security challenges (Mavroeidakos et al., 2022).

II. LITERATURE REVIEW

2.1 Healthcare IoT Ecosystem and Associated Risks

Healthcare IoT ecosystems encompass diverse device categories that serve distinct clinical functions while sharing common connectivity characteristics. Patient monitoring devices collect vital signs and physiological parameters continuously, transmitting data to electronic health record systems and triggering clinical alerts when measurements exceed defined thresholds. Therapeutic devices including infusion pumps and ventilators deliver medications and respiratory support under automated control responding to patient conditions. Diagnostic equipment generates medical imaging and laboratory results that inform treatment decisions. Implantable devices such as pacemakers and insulin pumps operate autonomously within patients' bodies while maintaining wireless connectivity for programming and data retrieval (Abdulmalek et al., 2022).

Each device category introduces specific vulnerability profiles shaped by operational requirements, technical architectures, and clinical integration patterns. Patient monitoring devices often transmit sensitive health data without encryption, exposing information to interception and unauthorized access. Therapeutic devices accept control commands that adversaries could manipulate to deliver incorrect treatments. Diagnostic equipment may contain patient data stored insecurely on local storage. Implantable devices present unique risks where remote exploitation could directly threaten patient safety through unauthorized device reprogramming (Ghubaish et al., 2021).

Research has documented numerous attack vectors exploiting healthcare IoT vulnerabilities. Network-based attacks leverage weak authentication protocols, unencrypted communications, and excessive device permissions to gain unauthorized access. Physical attacks target devices during maintenance, allowing adversaries to install hardware implants or extract cryptographic keys. Supply chain attacks compromise devices before deployment through malicious firmware, counterfeit components, or unauthorized modifications during distribution and integration (Ghubaish et al., 2021).

Clinical workflows compound security challenges by prioritizing availability and usability over security controls. Healthcare providers require immediate device access during emergencies, discouraging implementations of strong authentication that could delay treatment. Device manufacturers prioritize regulatory compliance and clinical functionality over cybersecurity features. These competing priorities create environments where security measures often receive secondary consideration despite recognized vulnerabilities (Thomasian & Adashi, 2021).

2.2 Medical Device Supply Chain Vulnerabilities

Medical device supply chains present multifaceted vulnerabilities spanning manufacturing, distribution, integration, and maintenance phases. At the manufacturing stage, counterfeit components represent a sophisticated threat where adversaries produce fake electronic parts that appear functionally equivalent to genuine components but contain hidden backdoors or degraded reliability. Component authentication proves challenging because counterfeits may incorporate legitimate serial numbers obtained through theft or insider access. Testing protocols typically verify functional specifications without detecting malicious circuitry designed to activate through specific triggers (Kioskli et al., 2022).

Firmware vulnerabilities emerge during development and persist throughout device lifecycles. Manufacturers may implement insecure coding practices, fail to validate third-party libraries, or neglect cryptographic signing of firmware updates. Build processes present opportunities for malicious insiders to inject backdoors or modify security functions. Post-manufacturing firmware distribution channels often lack integrity verification, enabling adversaries to substitute malicious firmware that devices accept as legitimate (Thomasian & Adashi, 2021).

Distribution and logistics present additional vulnerability points. Devices in transit may be intercepted and modified before reaching healthcare facilities. Warehouse storage exposes devices to tampering by employees or contractors with physical access. Integration processes often involve third-party contractors who configure devices for specific clinical environments, creating opportunities for intentional vulnerability introduction. Maintenance and servicing activities require technician access that may not receive adequate monitoring (Kioskli et al., 2022).

Third-party ecosystem exposure amplifies supply chain risks. Medical devices increasingly rely on external cloud services, remote monitoring platforms, and data analytics providers. Each third-party relationship introduces dependencies where compromise of external systems could affect connected medical devices. Software supply chains involving development tools, libraries, and frameworks present additional attack surfaces where adversaries compromise widely used components to affect multiple device models simultaneously.

The complexity of modern medical devices exacerbates supply chain vulnerabilities. Devices incorporate multiple software components, operating systems, communication protocols, and security features that interact in complex ways. Understanding the complete attack surface requires visibility across hardware, firmware, software, and network layers. Supply chain security demands mechanisms for verifying authenticity and integrity across all these dimensions throughout the device lifecycle (Thomasian & Adashi, 2021).

2.3 Zero Trust Security in Healthcare

Zero Trust architecture fundamentally challenges traditional security paradigms by eliminating implicit trust assumptions. The core principle of "never trust, always verify" requires continuous authentication and authorization for all access requests regardless of network location or previous authorization. Rather than granting broad network access after initial authentication, Zero Trust enforces least-privilege access where entities receive only minimal permissions required for specific tasks. This approach assumes breach and designs security controls to limit damage from compromised credentials or systems (Adahman et al., 2022).

Application of Zero Trust principles to healthcare IoT environments addresses several fundamental security challenges. Device identity becomes the foundation for access decisions, with each medical device possessing unique cryptographic credentials verified continuously throughout operations. Network segmentation limits device exposure by isolating medical devices within dedicated zones with strictly controlled communication paths. Micro-segmentation policies specify exactly which network resources each device type may access, preventing lateral movement by adversaries who compromise individual devices (Ali et al., 2021).

Implementation of Zero Trust in healthcare requires adaptation to clinical realities. Emergency scenarios demand immediate access to critical devices, necessitating pre-authorized access pathways that maintain security while accommodating urgent clinical needs. Legacy devices lacking modern authentication capabilities require overlay solutions providing Zero Trust enforcement without device modifications. Policy engines must balance security rigor with operational flexibility, applying risk-based authentication that escalates requirements when behavioral analytics detect anomalies (Chen et al., 2021).

Research demonstrates that Zero Trust architectures reduce attack surfaces and improve threat detection capabilities. By enforcing strict access controls and monitoring all device interactions, Zero Trust implementations detect unauthorized activities that perimeter-based security would miss. Comprehensive audit logging generated by Zero Trust enforcement provides forensic data supporting incident investigation and compliance reporting. The explicit verification requirements make it significantly harder for adversaries to move laterally within networks even after initial compromise (Sultana et al., 2020).

Several challenges impede Zero Trust adoption in healthcare environments. Legacy medical devices lack built-in support for modern authentication protocols, requiring overlay solutions that add complexity. Healthcare IT organizations often lack expertise and resources for Zero Trust implementation and ongoing management. Clinical workflows prioritizing rapid access may conflict with Zero Trust verification requirements. Addressing these challenges requires phased implementation approaches that begin with highest-risk devices while building organizational capabilities for broader deployment (Ferretti et al., 2021).

2.4 Role of AI in IoT Security and Vulnerability Detection

Artificial intelligence technologies provide powerful capabilities for addressing healthcare IoT security challenges through pattern recognition, behavioral analysis, and predictive modeling. Machine learning algorithms trained on large datasets of device behaviors and network traffic identify subtle anomalies indicating potential compromises that would escape manual analysis. Natural language processing extracts actionable intelligence from vast quantities of security advisories, vulnerability disclosures, and threat reports. Predictive analytics forecast which devices face elevated risk based on characteristics, vulnerabilities, and threat landscape evolution (Pise et al., 2022).

Behavioral profiling represents a key AI application for medical device security. AI systems establish baseline behavior patterns for individual devices by analyzing normal operational characteristics including communication frequencies, data volumes, protocol usage, and timing relationships. These behavioral fingerprints enable detection of counterfeit devices exhibiting subtle differences from genuine devices despite appearing functionally equivalent. Compromised devices executing malicious code typically exhibit behavioral deviations from established baselines, triggering alerts for security investigation (Pise et al., 2022).

Anomaly detection algorithms identify unusual patterns within healthcare IoT ecosystems that may indicate supply chain compromises or active attacks. Unsupervised learning techniques detect novel attack patterns without requiring prior examples of specific attack types. Statistical analysis identifies outliers representing devices with characteristics diverging significantly from population norms. Time-series analysis detects temporal anomalies including unexpected communication patterns or irregular data exfiltration. Graph analytics identify abnormal relationship patterns between devices, users, and network resources (Said et al., 2021).

Predictive risk scoring enables proactive vulnerability management by forecasting which devices face elevated compromise risk based on multiple factors. AI models incorporate device characteristics, vulnerability databases, threat intelligence, and historical incident data to identify complex relationships predicting future compromise likelihood. These quantitative risk scores enable prioritization of limited remediation resources toward highest-risk devices, improving overall security posture efficiency (Pise et al., 2022).

Natural language processing enhances threat intelligence by automatically analyzing vulnerability advisories, security bulletins, and threat reports to extract actionable information relevant to deployed devices. Automated systems identify relationships between vulnerabilities, threat actors, and attack techniques, enabling rapid assessment of organizational exposure when new vulnerabilities emerge. This automation accelerates patch deployment and risk mitigation decisions (Ngueajio et al., 2022).

Despite these powerful capabilities, AI implementations face challenges in healthcare environments. Training machine learning models requires substantial quantities of labeled data that may not be available for all device types or attack scenarios. Models trained on limited datasets may produce false positives disrupting clinical operations or false negatives missing actual threats. Adversarial attacks can manipulate AI systems through carefully crafted inputs that evade detection. Addressing these limitations requires ongoing model refinement, validation against diverse data sources, and human oversight of AI-generated recommendations (Qiu et al., 2022).

2.5 Identified Gaps in Current Literature

Existing literature addresses AI applications and Zero Trust principles independently but lacks comprehensive frameworks integrating these complementary approaches for medical device supply chain security. While research documents AI capabilities for anomaly detection and behavioral profiling, these studies typically examine AI in isolation without considering how Zero Trust enforcement mechanisms could enhance AI effectiveness through improved data quality and validation (Collier & Sarkis, 2021). Supply chain security research tends to concentrate on manufacturing and distribution vulnerabilities without adequately addressing the ongoing operational phase where continuous monitoring and verification prove essential. Literature examining counterfeit detection or firmware integrity often focuses on point-in-time assessments rather than persistent lifecycle security. This gap leaves healthcare organizations without guidance for maintaining supply chain security after initial device deployment (Collier & Sarkis, 2021).

Few studies examine the synergies between AI and Zero Trust, particularly how AI-generated behavioral insights inform Zero Trust access decisions and how Zero Trust architectures generate data streams enhancing AI model training. Understanding these integration points could demonstrate how complementary technologies create security capabilities exceeding what either approach provides independently. This research addresses these gaps by proposing an integrated framework leveraging both AI and Zero Trust strengths for comprehensive medical device supply chain security (Li et al., 2022).

III. THEORETICAL FRAMEWORK

3.1 Zero Trust Architecture Model

The Zero Trust model establishes a security paradigm fundamentally opposed to traditional perimeter-based approaches. Rather than assuming trust based on network location, Zero Trust requires continuous verification of device identity, user credentials, and contextual attributes for every access request. This model eliminates the concept of trusted internal networks, instead treating all network traffic as potentially hostile regardless of origin. The architecture enforces least-privilege access where entities receive only minimal permissions required for specific tasks, with authorizations reassessed continuously rather than granted indefinitely after initial authentication (Adahman et al., 2022).

For medical device supply chains, Zero Trust architecture provides critical capabilities for maintaining security throughout the device lifecycle. During procurement, Zero Trust principles require verification of device authenticity through cryptographic attestation before granting network access. Throughout operations, continuous device identity validation detects situations where devices become compromised after deployment. Network segmentation limits exposure by isolating devices within dedicated zones with strictly controlled communication paths. Verified firmware updates with cryptographic validation prevent unauthorized software modifications. Comprehensive audit logging documents all device activities, supporting forensic investigations and compliance reporting (Køien, 2021).

The Zero Trust model addresses supply chain vulnerabilities through several core components. Device identity serves as the foundation, with each medical device possessing unique cryptographic credentials anchored in hardware-based roots of trust resistant to cloning. Policy enforcement points evaluate access requests against defined security policies considering device identity, user credentials, requested resources, behavioral patterns, and environmental context. Dynamic policies adapt to changing risk levels, requiring additional authentication or restricting access when anomalies arise. Micro-segmentation prevents lateral movement by specifying exactly which network resources each device may access (Tyler & Viana, 2021).

Implementation of Zero Trust for medical devices requires policy enforcement points that evaluate access requests against defined security policies. These enforcement points examine multiple attributes simultaneously including device identity, user credentials, requested resources, current threat intelligence, and behavioral indicators. Access decisions occur in real-time based on comprehensive risk assessment rather than static rules. Failed authorization attempts trigger automated responses including network isolation, alert generation, and access revocation. This continuous verification ensures that compromised devices cannot maintain network access even if initial authentication succeeded (Chen et al., 2021).

3.2 AI-Driven Cyber Risk Decision Model

AI technologies enhance cybersecurity decision-making through automated analysis, pattern recognition, and predictive modeling that exceed human analytical capabilities. The AI-driven risk decision model processes vast quantities of data from diverse sources to identify threats, assess risks, and recommend response actions. Machine learning algorithms detect subtle patterns across device populations that would escape manual analysis. Natural language processing extracts structured information from unstructured threat intelligence. Predictive analytics forecast future risks based on historical trends and current indicators (Aledhari et al., 2022).

The model operates through several integrated components. Data collection mechanisms gather information from medical devices, network infrastructure, security tools, and external threat feeds. Feature engineering transforms raw data into meaningful attributes suitable for analysis. Machine learning models trained on diverse datasets identify behavioral baselines, detect anomalies, assess firmware integrity, and predict compromise risks. Decision logic translates model outputs into actionable recommendations for security teams or automated response systems (Hady et al., 2020).

Predictive capabilities enable proactive vulnerability management by forecasting which devices face elevated compromise risk before attacks occur. AI models analyze historical incident data, vulnerability disclosures, threat intelligence, and device characteristics to identify complex patterns associated with successful compromises. These predictions prioritize remediation activities toward highest-risk devices, optimizing allocation of limited security resources. Continuous risk reassessment adapts to evolving threats and changing device populations (Hady et al., 2020).

The AI model supports continuous learning and adaptation as new threats emerge and attack techniques evolve. Feedback loops incorporate incident outcomes to refine model accuracy over time. Transfer learning enables knowledge gained from one device type or healthcare organization to benefit others facing similar threats. Ensemble methods combine multiple analytical techniques to improve overall detection accuracy and reduce false positives (Susilo & Sari, 2020).

Integration between AI and Zero Trust creates synergistic effects where each approach enhances the other. AI-generated risk scores inform Zero Trust access decisions, with high-risk devices receiving elevated scrutiny or temporary access restrictions. Zero Trust audit logs provide ground truth data for training AI models, improving detection accuracy through labeled examples of legitimate and suspicious activities. This bidirectional relationship creates continuously improving security posture exceeding static controls (Hady et al., 2020).

IV. METHODOLOGY

4.1 Research Design

This study employs an exploratory and descriptive qualitative research approach to examine the integration of AI capabilities and Zero Trust principles for medical device supply chain security. The exploratory component investigates emerging technologies and their potential applications to address identified security gaps. The descriptive component documents current supply chain vulnerabilities, existing security controls, and regulatory requirements shaping healthcare cybersecurity. Qualitative methodology provides appropriate tools for examining complex sociotechnical systems where human factors, organizational processes, and technical architectures interact in ways that resist purely quantitative analysis. The research follows a structured process beginning with comprehensive literature review to establish theoretical foundations and identify existing knowledge gaps. Analysis of regulatory guidance and industry standards documents requirements and best practices. Synthesis of findings produces an integrated framework combining AI and Zero Trust capabilities for comprehensive supply chain security.

4.2 Data Sources

This research draws upon multiple authoritative sources to ensure comprehensive coverage of medical device supply chain security topics. Peer-reviewed academic journals provide theoretical foundations and empirical findings regarding IoT security, supply chain vulnerabilities, Zero Trust architectures, and AI applications (Elsayed et al., 2022). Conference proceedings document emerging technologies and novel approaches before formal publication. Technical reports from cybersecurity organizations detail attack techniques, vulnerability analyses, and defense mechanisms.

Cybersecurity advisory publications from organizations including the Cybersecurity and Infrastructure Security Agency (CISA), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and sector-specific information sharing organizations provide real-world threat intelligence. Vulnerability databases document disclosed security flaws affecting medical devices. Incident reports describe actual compromises and lessons learned from security breaches (Alshehri & Muhammad, 2021).

Regulatory guidance from the Food and Drug Administration (FDA) establishes baseline security expectations for medical device manufacturers and healthcare organizations. FDA premarket cybersecurity guidance, post-market management directives, and safety communications define regulatory requirements shaping device development and deployment. National Institute of Standards and Technology (NIST) frameworks provide structured approaches to cybersecurity risk management applicable across sectors (Alshehri & Muhammad, 2021).

Industry standards from organizations including the Health Information Trust Alliance (HITRUST), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC) establish technical specifications and best practices. These standards address device security, network architecture, risk assessment, and security controls implementation. Medical device manufacturer security documentation provides insights into actual implementation challenges and capabilities (Elsayed et al., 2022).

4.3 Analysis Technique

The research employs thematic synthesis as the primary analysis technique, systematically identifying patterns, relationships, and themes across diverse information sources. This approach enables integration of findings from academic literature, technical reports, regulatory guidance, and industry documentation to develop comprehensive understanding of supply chain security challenges and potential solutions (Naz et al., 2022).

Analysis proceeds through several stages. Initial coding identifies relevant concepts including specific vulnerabilities, attack techniques, security controls, and implementation challenges. Descriptive themes organize related concepts into broader categories representing major vulnerability areas, AI capabilities, and Zero Trust mechanisms. Analytical themes examine relationships between concepts, identifying how specific AI techniques address particular vulnerabilities and how Zero Trust controls complement AI capabilities (Naz et al., 2022).

The synthesis process explicitly examines relationships between AI capabilities and Zero Trust principles, identifying complementary functions and potential integration points. Analysis maps specific supply chain vulnerabilities to AI detection techniques and Zero Trust controls addressing those weaknesses. This mapping reveals gaps where neither approach provides adequate protection independently but integration creates comprehensive defense (Belhadi et al., 2021).

Framework development represents the culminating analysis activity, organizing identified themes, relationships, and recommendations into a structured model that healthcare organizations can implement. The framework specifies roles for different stakeholders including healthcare facilities, device manufacturers, and regulatory bodies. Implementation guidance addresses technical requirements, resource considerations, and phased deployment strategies accommodating varying organizational capabilities (Naz et al., 2022).

Quality assurance mechanisms ensure analysis validity and reliability. Multiple information sources provide triangulation that strengthens findings by confirming patterns across different data types. Systematic documentation of analysis decisions creates audit trails supporting transparency. Attention to conflicting evidence prevents overstating conclusions or ignoring limitations (Pavlov et al., 2022).

V. RESULTS AND FINDINGS

5.1 Summary of Supply Chain Weaknesses Identified

Analysis reveals four critical vulnerability categories affecting medical device supply chains: firmware manipulation, counterfeit components, vulnerable distribution and logistics, and inconsistent update and patch mechanisms. Each category presents distinct attack vectors while contributing to systemic supply chain risks that adversaries exploit for device compromise (Brady et al., 2020). The following table summarizes these vulnerabilities:

Table 1: Critical Supply Chain Vulnerability Categories

Vulnerability Category	Attack Vectors	Impact	Detection Challenges
Firmware Manipulation	Insecure coding practices, malicious third-party libraries, backdoor injection during compilation, malicious firmware substitution during updates	Complete device compromise, unauthorized access to patient data, potential for remote device manipulation	Difficult to detect without cryptographic verification and baseline comparison
Counterfeit Components	Hardware trojans in fake integrated circuits, degraded component reliability, legitimate serial number forgery	Hidden backdoors enabling persistent access, time-delayed device failures, covert data exfiltration	Functional testing insufficient to detect malicious circuitry; legitimate serial numbers complicate authentication
Distribution & Logistics Vulnerabilities	Physical device tampering during transit, hardware implant installation, insider threats in warehouses, unauthorized modifications during integration	Pre-deployment compromise of device integrity, persistent backdoors established before clinical use	Limited supply chain visibility prevents detection of tampering; lack of continuous monitoring during distribution
Inconsistent Update & Patch Mechanisms	Manual update processes requiring clinical downtime, lack of automated patch deployment, inconsistent authentication for updates, absence of patches for legacy devices	Prolonged vulnerability exposure to known exploits, fragmented device fleet with inconsistent security postures	Difficult to track patch status across device populations; clinical priorities delay security updates

The identified vulnerabilities share common characteristics that facilitate exploitation. Insufficient visibility prevents healthcare organizations from detecting compromised devices or components before deployment. Limited validation mechanisms allow malicious modifications to proceed without detection. Weak authentication enables adversaries to impersonate legitimate suppliers, integrators, or service providers. These systemic weaknesses mean that resolving individual vulnerabilities provides incomplete protection without addressing underlying supply chain security shortcomings (Sfalionis et al., 2022).

5.2 How AI Techniques Address These Weaknesses

Artificial intelligence provides multiple capabilities that directly address identified supply chain vulnerabilities through behavioral profiling, anomaly detection, firmware integrity analysis, and predictive risk scoring. These AI techniques operate continuously throughout the device lifecycle, providing persistent security monitoring that adapts to evolving threats (Al-Garadi et al., 2020). The following table maps specific AI techniques to the vulnerabilities they address:

Table 2: AI Techniques Mapped to Supply Chain Vulnerabilities

AI Technique	Primary Function	Addresses Vulnerabilities	Key Capabilities
Behavioral Profiling	Establish baseline operational patterns for individual devices through network traffic and resource utilization analysis	Counterfeit device detection, compromised device identification through behavioral deviations	Network traffic analysis, communication frequency patterns, protocol usage fingerprinting, timing relationship identification
Anomaly Detection	Identify unusual patterns within healthcare IoT ecosystems indicating potential attacks or compromises	Supply chain attacks, active exploitation detection, novel attack pattern identification	Unsupervised learning for novel threats, statistical outlier detection, time-series temporal analysis, graph analytics for relationship patterns
Firmware Integrity Analysis	Detect unauthorized firmware modifications through comparison against known-good baselines	Firmware manipulation prevention, malicious code injection detection	Static code analysis for suspicious patterns, dynamic behavior monitoring, NLP metadata analysis, ML-based modification classification
Predictive Risk Scoring	Forecast which devices face elevated compromise risk through multi-source data synthesis	Proactive vulnerability management across all vulnerability categories	Multi-factor risk model incorporating device characteristics, vulnerability databases, threat intelligence, historical incident analysis

AI Technique	Primary Function	Addresses Vulnerabilities	Key Capabilities
Threat Intelligence Automation	Accelerate vulnerability response through automated analysis of security advisories and threat reports	All vulnerability categories through rapid threat assessment and patch prioritization	NLP for advisory parsing, entity recognition for vulnerability mapping, knowledge graphs for threat relationships

Integration of these AI techniques creates layered defense capabilities exceeding individual components. Behavioral profiling provides early warning of potential compromises that anomaly detection confirms through multiple analytical perspectives, while firmware integrity analysis validates whether detected anomalies reflect actual tampering rather than benign operational changes (Shu et al., 2022). Predictive risk scoring focuses limited analytical resources on highest-priority threats, and automated threat intelligence processing supports rapid assessment of new advisories and exploits (Al-Garadi et al., 2020). This integrated approach addresses supply chain vulnerabilities comprehensively while managing alert fatigue through correlation and validation mechanisms (Radanliev & De Roure, 2022).

5.3 How Zero Trust Controls Strengthen the Device Lifecycle

Zero Trust architecture addresses supply chain vulnerabilities through continuous validation of device identity, network segmentation that limits device exposure, verified updates with controlled access, and comprehensive audit logging throughout the device lifecycle. These controls operate from procurement through retirement, providing persistent security enforcement that adapts to changing risk levels (Liu et al., 2022). The following table demonstrates how Zero Trust controls map to lifecycle stages:

Table 3: Zero Trust Controls Across Device Lifecycle Stages

Zero Trust Control	Implementation Mechanism	Lifecycle Stage	Supply Chain Vulnerability Addressed
Continuous Device Identity Validation	Cryptographic attestation through challenge-response protocols, hardware-based roots of trust, continuous verification beyond initial authentication	Deployment through Operations	Counterfeit device detection, post-deployment compromise identification, unauthorized device prevention
Network Segmentation	Micro-segmentation policies specifying authorized communications, VLANs separating device traffic,	Operations	Lateral movement prevention, breach containment, exposure

Zero Trust Control	Implementation Mechanism	Lifecycle Stage	Supply Chain Vulnerability Addressed
	software-defined networking for dynamic adaptation		limitation for compromised devices
Verified Firmware Updates	Digital signatures proving update authenticity, secure boot validation, encrypted update channels with certificate pinning, controlled update privileges	Operations through Maintenance	Firmware manipulation prevention, man-in-the-middle attack protection, unauthorized update blocking
Comprehensive Audit Logging	Detailed activity records with device identity, requested resources, timestamps, centralized log aggregation, immutable storage using blockchain or WORM media	All Stages	Forensic investigation support, compliance reporting, attack pattern identification, adversary track covering prevention
Dynamic Policy Enforcement	Policy engines evaluating access requests against rules, risk-based authentication requiring additional verification, emergency access pathways, policy testing environments	All Stages	Consistent security across heterogeneous devices, adaptive response to risk changes, clinical workflow accommodation

Zero Trust controls address specific supply chain vulnerabilities through targeted mechanisms. Counterfeit device detection occurs through device identity verification that reveals devices lacking valid manufacturer credentials. Firmware manipulation prevention employs verified updates requiring cryptographic signatures. Unauthorized access attempts by compromised devices fail due to continuous authentication requirements. Distribution channel attacks become ineffective because devices must prove identity regardless of physical possession. These targeted controls complement AI-driven detection capabilities to create defense-in-depth protecting against diverse attack vectors (Mushtaq et al., 2022).

5.4 Combined Insights: AI Supports Visibility and Prediction While Zero Trust Enforces Verification and Control

Integration of AI capabilities with Zero Trust controls creates synergistic effects where complementary strengths address medical device supply chain security more comprehensively than either approach independently. AI provides visibility through continuous monitoring, pattern recognition through behavioral analytics, and prediction through risk modeling. Zero Trust enforces verification through continuous authentication, control through policy enforcement, and containment through network segmentation. Together, these approaches create layered defenses operating at detection and prevention levels simultaneously (Collier & Sarkis, 2021).

The following table illustrates key integration points where AI and Zero Trust components work synergistically:

Table 4: AI and Zero Trust Integration Matrix

Integration Point	AI Component	Zero Trust Component	Combined Effect
Risk-Based Access Control	Behavioral risk scoring analyzing device activities and threat indicators	Dynamic policy enforcement requiring additional authentication for high-risk devices	Real-time access decisions based on continuous device behavior assessment, automatically escalating security requirements when anomalies detected
Enhanced Detection Accuracy	Machine learning model training requiring labeled ground truth data	Comprehensive audit logs documenting legitimate and suspicious device activities	Zero Trust logs provide high-quality training data improving AI model accuracy, reducing false positives through validated examples of normal behavior
Automated Incident Response	Anomaly detection identifying compromised devices through behavioral deviations	Network isolation mechanisms triggered automatically for suspicious devices	AI-detected anomalies trigger immediate Zero Trust quarantine, containing threats before lateral movement while security teams investigate
Procurement Security Validation	Supplier risk analysis evaluating security practices and component authenticity	Device identity verification requirements before network authorization	AI supplier assessment informs Zero Trust onboarding policies, with high-risk vendors requiring enhanced device validation before deployment
Continuous Lifecycle Monitoring	Predictive risk models forecasting device compromise likelihood	Continuous authentication requiring ongoing identity verification	AI risk predictions trigger proactive Zero Trust authentication frequency increases, catching compromises early through mandatory re-verification

The combined framework addresses supply chain vulnerabilities through multiple defense layers operating at different lifecycle stages. During procurement, AI analysis of supplier security practices and component provenance informs Zero Trust onboarding requirements. Throughout operations, AI behavioral analytics detect anomalies that Zero Trust policies use to adjust access privileges dynamically. During maintenance, verified firmware updates combine cryptographic Zero Trust validation with AI integrity analysis detecting unauthorized modifications. This comprehensive approach ensures that compromises at any lifecycle stage face multiple overlapping defenses rather than single points of failure (Collier & Sarkis, 2021).

VI. CONCLUSION

This research establishes that integrating artificial intelligence capabilities with Zero Trust security principles creates a comprehensive framework addressing critical vulnerabilities in medical device supply chains throughout device lifecycles. The analysis identifies four major vulnerability categories firmware manipulation, counterfeit components, distribution vulnerabilities, and inconsistent update mechanisms that expose healthcare organizations to sophisticated supply chain attacks compromising device integrity before deployment. Traditional security controls focusing on perimeter defense prove insufficient against these threats that bypass network boundaries entirely.

The proposed integrated framework demonstrates how AI and Zero Trust approaches complement each other through distinct yet synergistic functions. AI provides continuous monitoring, behavioral profiling, anomaly detection, firmware integrity analysis, and predictive risk scoring that enhance visibility into device states and threat landscapes. Zero Trust enforces continuous authentication, network segmentation, verified updates, comprehensive audit logging, and dynamic policy enforcement that prevent and contain compromises. Together, these capabilities create defense-in-depth protecting against diverse attack vectors while accommodating clinical operational requirements.

Implementation of the framework requires careful consideration of healthcare operational requirements, regulatory compliance obligations, and technical constraints specific to medical devices. The research provides actionable guidance for hospitals establishing device inventories, deploying continuous monitoring, and implementing incident response procedures. Recommendations for manufacturers emphasize security-by-design principles, component authentication, and cryptographic update mechanisms. Regulatory considerations address minimum security requirements, implementation incentives, and information sharing initiatives. This multi-stakeholder approach recognizes that supply chain security demands coordinated action across the healthcare ecosystem.

The framework's significance extends beyond immediate security improvements to support broader healthcare cybersecurity maturity. By implementing AI-enhanced monitoring and Zero Trust verification, organizations develop capabilities applicable to other connected medical technologies and critical infrastructure. The integration model demonstrates how emerging technologies address long-standing vulnerabilities when deployed strategically with complementary controls. As healthcare IoT ecosystems continue expanding, frameworks combining multiple defensive approaches will prove essential for maintaining security without compromising the clinical innovations these technologies enable.

Future research should examine empirical validation of the framework through pilot implementations within healthcare organizations, measuring security outcomes, operational impacts, and resource requirements. Longitudinal studies could assess how integrated AI and Zero Trust approaches evolve as threat landscapes change and technologies mature. Comparative analysis across healthcare organizations with varying resource levels could identify implementation patterns supporting broader adoption. Investigation of adversary responses to these defensive measures would inform ongoing framework refinement ensuring continued effectiveness against sophisticated supply chain attacks.

7. RECOMMENDATIONS

Implementation of the AI-driven Zero Trust framework requires coordinated action across multiple stakeholders in the healthcare IoT ecosystem. The following recommendations provide specific guidance for hospitals and healthcare facilities, medical device manufacturers, and policymakers and regulators. Each stakeholder group plays distinct roles in strengthening supply chain security while contributing to comprehensive protection across device lifecycles (Kioskli et al., 2022).

Table 5: Stakeholder Recommendations for Framework Implementation

Stakeholder	Priority Actions	Technical Requirements	Expected Outcomes
Hospitals & Healthcare Facilities	• Establish comprehensive device inventories documenting all connected devices • Implement network segmentation isolating medical devices • Deploy AI-driven continuous monitoring for anomalous activities • Develop incident response procedures for device compromises • Establish secure firmware update processes with manufacturers	• SIEM platform integration • Behavioral analytics capabilities • Cryptographic attestation systems • Micro-segmentation infrastructure • Tabletop exercise programs • Compensating controls for legacy devices	• Complete device visibility across clinical environments • Reduced attack surface through network isolation • Faster compromise detection and response • Regulatory compliance achievement • Systematic vulnerability remediation
Medical Device Manufacturers	• Implement security-by-design throughout product lifecycles • Establish supply chain security programs for component authentication • Develop cryptographically signed update mechanisms • Provide comprehensive product security documentation • Support legacy devices with security patches throughout lifecycles	• Threat modeling tools • Hardware roots of trust implementation • Over-the-air update capabilities • Automated security analysis in development • Blockchain-based provenance tracking • Information sharing participation	• Reduced product vulnerabilities from inception • Supply chain integrity verification • Rapid vulnerability patch deployment • Enhanced customer trust through transparency • Regulatory compliance demonstration
Policymakers & Regulators	• Mandate minimum security requirements throughout device lifecycles	• Enhanced premarket security review • Post-market surveillance systems	• Industry-wide minimum security baselines

Stakeholder	Priority Actions	Technical Requirements	Expected Outcomes
	• Provide implementation incentives through funding and safe harbors • Establish confidential information sharing frameworks • Harmonize regulations across jurisdictions • Develop cybersecurity workforce programs	• Interoperability standards development • International cooperation mechanisms • Training and certification programs • Liability protection for disclosure	• Accelerated threat response through coordination • Transparent vulnerability disclosure • Global supply chain security standards • Expanded cybersecurity expertise in healthcare sector

These recommendations recognize that supply chain security requires coordinated action across the healthcare ecosystem. Hospitals must implement technical controls while managing operational constraints. Manufacturers must embed security throughout product development while maintaining clinical functionality. Regulators must establish requirements while accommodating diverse implementation approaches. Success depends on all stakeholders fulfilling their distinct responsibilities while collaborating to address shared challenges (Kioskli et al., 2022). The integrated AI and Zero Trust framework provides the technical foundation, but effective implementation demands sustained commitment from all parties to strengthen medical device security comprehensively (Rasool et al., 2022).

REFERENCES

[1] Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuhaya, M. A. M., Bairagi, A. K., Khan, M. A.-M., & Kee, S.-H. (2022). IoT-based healthcare-monitoring system towards improving quality of life: A review. *Healthcare, 10*(10), 1993. https://doi.org/10.3390/healthcare10101993

[2] Adahman, Z., Malik, A. W., & Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security, 122*, 102911. https://doi.org/10.1016/j.cose.2022.102911

[3] Aledhari, M., Razzak, R., Qolomany, B., Al-Fuqaha, A., & Saeed, F. (2022). Biomedical IoT: Enabling technologies, architectural elements, challenges, and future directions. *IEEE Access, 10*, 31306–31339. 10.1109/ACCESS.2022.3159235

[4] Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Communications Surveys & Tutorials, 22*(3), 1646–1685. https://doi.org/10.1109/COMST.2020.2988293

[5] Ali, B., Gregory, M. A., & Li, S. (2021). Uplifting Healthcare Cyber Resilience with a Multi-access Edge Computing Zero-Trust Security model. *2021 31st International Telecommunication Networks and Applications Conference (ITNAC)*, 192–197. https://doi.org/10.1109/itnac53136.2021.9652141

[6] Alshehri, F., & Muhammad, G. (2021). A comprehensive survey of the internet of things (IOT) and AI-based Smart Healthcare. *IEEE Access*, *9*, 3660–3678. https://doi.org/10.1109/access.2020.3047960

[7] Baker, S. D. (2022). The ironic state of cybersecurity in medical devices. *Biomedical Instrumentation & Technology, 56*(3), 98–101. https://doi.org/10.2345/0899-8205-56.3.98

[8] Belhadi, A., Kamble, S. S., Jabbour, C. J. C., Gunasekaran, A., Ndubisi, N. O., & Venkatesh, M. (2021). Artificial intelligence-driven supply chain resilience: A systematic literature review

and a research agenda. *International Journal of Production Research, 59*(7), 2100–2123. https://doi.org/10.1080/00207543.2020.1824084

[9] Brady, E., Loseke, T., Potts, J., & Yuan, B. (2020). Securing the medical device supply chain: A systematic literature review. *IEEE Access, 8*, 209783–209800. https://doi.org/10.1109/ACCESS.2020.3038472

[10] Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., & Zhai, Y. (2021). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, *8*(13), 10248–10263. https://doi.org/10.1109/jiot.2020.3041042

[11] Collier, Z. A., & Sarkis, J. (2021). The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research, 59*(11), 3430–3445. https://doi.org/10.1080/00207543.2021.1884311

[12] Elsayed, N., Abdelgawad, A., & Elsayed, Z. (2022). Cybersecurity and frequent cyber attacks on IoT devices in healthcare: Issues and solutions. *IEEE Access, 10*, 110802–110829. https://doi.org/10.1109/ACCESS.2022.3200213

[13] Ferretti, L., Marchetti, M., & Andreolini, M. (2021). Survivable zero trust for cloud computing environments. *Computers & Security, 103*, 102171. https://doi.org/10.1016/j.cose.2021.102171

[14] Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2021). Recent advances in the internet-of-medical-things (IOMT) systems security. *IEEE Internet of Things Journal*, *8*(11), 8707–8718. https://doi.org/10.1109/jiot.2020.3045653

[15] Hady, A. A., Ghubaish, A., Salman, T., Unal, D., & Jain, R. (2020). Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access*, *8*, 106576–106584. https://doi.org/10.1109/access.2020.3000421

[16] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of Medical Internet Research, 23*(4), e21747. https://doi.org/10.2196/21747

[17] Kioskli, K., Grigoriou, E., Islam, S., Yiorkas, A. M., Christofi, L., & Mouratidis, H. (2022). A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain. *International Journal of Information Security, 21*(6), 1339–1360. https://doi.org/10.1007/s10207-021-00587-4

[18] Køien, G. M. (2021). Zero-trust principles for legacy components: 12 rules for legacy devices—An antidote to chaos. *Wireless Personal Communications, 121*(2), 1169–1186. https://doi.org/10.1007/s11277-021-09055-1

[19] Li, S., Iqbal, M., & Saxena, N. (2022). Future industry Internet of Things with zero-trust security. *Information Systems Frontiers, 24*(5), 1583–1596. https://doi.org/10.1007/s10796-021-10152-3

[20] Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., Liu, Y., & Liu, Q. (2022). Dissecting zero trust: Research landscape and its implementation in IoT. *Cybersecurity, 5*(1), 1–31. https://doi.org/10.1186/s42400-022-00110-2

[21] Markus, A. F., Kors, J. A., & Rijnbeek, P. R. (2021). The role of explainability in creating trustworthy artificial intelligence for health care: A comprehensive survey of the terminology, design choices, and evaluation strategies. *Journal of Biomedical Informatics, 113*, 103655. https://doi.org/10.1016/j.jbi.2020.103655

[22] Mavroeidakos, T., Georgiou, O., & Voulkidis, A. (2022). Zero trust based cybersecurity architecture for healthcare IoT using artificial intelligence. *IEEE Access, 10*, 75432–75445. https://doi.org/10.1109/ACCESS.2022.3187654

[23] Mushtaq, S., Mohsin, M., Mushtaq, M. M., & others. (2022). A systematic literature review on the implementation and challenges of zero trust architecture across domains. *Sensors, 22*(19), 1–30. https://doi.org/10.3390/s22197234

[24] Naz, F., Kumar, A., Majumdar, A., & Agrawal, R. (2022). Is artificial intelligence an enabler of supply chain resiliency post COVID-19? An exploratory state-of-the-art review for future research. *Operations Management Research, 15*(1–2), 378–398. https://doi.org/10.1007/s12063-021-00208-w

[25] Ngueajio, C., Bassirou, A. B., Abdou, A. G., & Ali, M. L. (2022). A comprehensive survey of intrusion detection systems using machine

learning for IoT and cyber–physical systems. *International Journal of Information Security and Privacy, 16*(3), 1–27. https://doi.org/10.4018/IJISP.310110

[26] Pavlov, A., Bharadwaj, S. S., & Vasilyeva, E. (2022). Zero trust architecture for healthcare cyber-physical systems: A systematic review of design principles and implementation challenges. *IEEE Access, 10*, 45701–45725. https://doi.org/10.1109/ACCESS.2022.3172105

[27] Pise, A. A., Almuzaini, K. K., Ahanger, T. A., Farouk, A., Pant, K., Pareek, P. K., & Nuagah, S. J. (2022). Enabling Artificial Intelligence of Things (AIoT) healthcare architectures and listing security issues. *Computational Intelligence and Neuroscience, 2022*, Article 8421434. https://doi.org/10.1155/2022/8421434

[28] Qiu, S., Liu, Q., Zhou, S., & Huang, W. (2022). Adversarial attack and defense technologies in Natural Language Processing: A Survey. *Neurocomputing*, *492*, 278–307. https://doi.org/10.1016/j.neucom.2022.04.020 3

[29] Radanliev, P., & De Roure, D. (2022). Advancing the cybersecurity of the healthcare system with self optimising and self adaptative artificial intelligence (part 2). *Health and Technology, 12*(5), 923–929. https://doi.org/10.1007/s12553-022-00691-6

[30] Rasool, R. U., Kausar, M. A., Shah, M. A., & Javaid, N. (2022). Health IoT threats: Survey of risks and vulnerabilities. *Future Internet, 14*(11), 389. https://doi.org/10.3390/fi14110389

[31] Said, A. M., Yahyaoui, A., & Abdellatif, T. (2021). Efficient anomaly detection for smart hospital IoT systems. *Sensors, 21*(4), 1026. https://doi.org/10.3390/s21041026

[32] Schwartz, S. M., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., Petrozzino, C., & Zuk, M. (2018). The evolving state of medical device cybersecurity. *Biomedical Instrumentation & Technology, 52*(2), 103–111. https://doi.org/10.2345/0899-8205-52.2.103

[33] Sfalionis, D., Kylilis, N., Gatzoulis, L., & Fysarakis, K. (2022). Cybersecurity risk management for medical devices and healthcare supply chains: Challenges and recommendations. *Health Policy and Technology, 11*(2), 100624. https://doi.org/10.1016/j.hlpt.2022.100624

[34] Shu, R., Zhang, K., Xiong, H., Wang, W., Zhu, H., & Zhang, Y. (2022). IoT device fingerprinting and abnormal behavior detection via deep learning. *IEEE Internet of Things Journal, 9*(10), 7164–7178. https://doi.org/10.1109/JIOT.2021.3119829

[35] Sultana, M., Hossain, A., Laila, F., Taher, K. A., & Islam, M. N. (2020). Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Medical Informatics and Decision Making, 20*(1), 266. https://doi.org/10.1186/s12911-020-01300-4

[36] Susilo, B., & Sari, R. F. (2020). Intrusion detection in IoT networks using deep learning algorithm. *Information, 11*(6), 279. https://doi.org/10.3390/info11060279

[37] Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. *Health Policy and Technology*, *10*(3), 100549. https://doi.org/10.1016/j.hlpt.2021.100549

[38] Tyler, D., & Viana, T. (2021). Trust no one? A framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. *Applied Sciences, 11*(16), 7356. https://doi.org/10.3390/app11167499