International Journal of Medical and All Body Health Research

IoT Device Security in Modern Healthcare: Addressing Cyber Threats to Connected Medical Equipment

Oghenemena Erukayenure [1*], Habeeb Abolaji Bashir [2], Ademola Adekunbi [3], Oluwafemi Samuel Esan [4], Oladimeji Idris Adeniji [5], Taiwo Dunsin Eyinfun [6]

[1] Department of Information Systems, Baylor University, Texas, USA
[2] Department of Statistics and Data Science, University of Kentucky, Kentucky, USA
[3] Department of Legal Services, Royal Marsden NHS Foundation Trust, London, UK
[4] Department of Data Analytics and Visualization, Morgan State University, Maryland, USA
[5] Department of Science and Technology, Bournemouth University, Bournemouth, UK
[6] Department of Computing and Informatics, University of Louisiana at Lafayette, Louisiana, USA

* Corresponding Author: **Oghenemena Erukayenure**

Article Info

ISSN (online): 2582-8940
Volume: 06
Issue: 04
October-December 2025
Received: 20-08-2025
Accepted: 21-09-2025
Published: 14-10-2025
Page No: 49-57

Abstract

The swift proliferation of Internet of Things (IoT) devices in healthcare, ranging from wearable monitors to interconnected infusion pumps, presents significant advantages while simultaneously posing critical cybersecurity threats. This study examines recent literature and documented case studies to pinpoint vulnerabilities in connected medical devices and suggest strategies for secure IoT healthcare. We use a thorough review of the literature and an analysis of published incident reports to group common attack vectors (like ransomware, data exfiltration, and denial-of-service) and find device vulnerabilities (like weak authentication, outdated firmware, and insecure protocols). We look at important countermeasures like encrypting data in transit, using zero-trust architectures, and using AI to find unusual patterns. Blockchain-based integrity checks and federated anomaly-detection models are two new solutions that are being talked about. The results combine advice from standards like HIPAA, GDPR, and NIST, and they stress the importance of layered security and lifecycle management. The conclusions underscore the ramifications for healthcare practice and policy, particularly the significance of device certification and staff training. They also propose future research avenues, including quantum-resilient cryptography and digital-twin simulations to anticipate IoT threats.

DOI: https://doi.org/10.54660/IJMBHR.2025.6.4.49-57

Keywords: IoT Security, Healthcare Cybersecurity, Connected Medical Devices, Cyber Threats, Patient Safety

Introduction

Connected medical devices (IoT-based wearables, smart pumps, telemedicine monitors, etc.) are increasingly prevalent in modern healthcare delivery. By 2030 it is estimated that ~50 billion IoT devices will be in use globally. Hospitals and clinics have embraced this connectivity for real-time patient monitoring, remote diagnostics, and automated care (e.g., automated insulin delivery). For instance, improved device networking can enable continuous glucose or cardiac rhythm tracking, feeding data to clinicians and patients alike. However, the attributes that make IoT valuable – pervasive connectivity and real-time data exchange – also open multiple cybersecurity attack vectors. The healthcare sector is now a frequent target: between 2013–2016, 93 networked-health incidents were reported, and by 2022 the average breach cost had reached $4.35 million. Unsecured medical equipment or compromised health records can directly endanger patients (e.g. by altering therapy delivery) and violate privacy laws.

Thus, gaps in IoT device security not only threaten data confidentiality and integrity but also patient safety and public trust.

This paper seeks to answer the following research questions (RQs): RQ1: What are the predominant cyber threats targeting IoT-enabled medical devices? RQ2: What security vulnerabilities (in design, deployment, or maintenance) do connected healthcare devices commonly exhibit? RQ3: What existing and emerging mitigation strategies (technical and organizational) can improve IoT medical device security? To address these questions, we conduct a structured literature review of Scopus-indexed research (past 5–7 years) supplemented by case studies from reputable reports. The analysis is oriented to U.S. healthcare context (regulatory and infrastructure), but lessons are broadly applicable. The paper is organized as follows: The Literature Review summarizes IoT adoption trends, known security challenges, and notable healthcare cyber incidents. The Theoretical Framework outlines applicable standards (e.g. NIST, HIPAA/GDPR) and the CIA security triad in the IoT healthcare setting. The Methodology describes our case-study and secondary-data approach. Results detail identified threat categories, lifecycle vulnerabilities, and effectiveness of countermeasures. The Discussion interprets these findings against prior work, addressing trade-offs, ethical/legal issues (e.g. patient privacy regulation), and implications for stakeholders. We conclude with recommendations for practice, policy, and future research.

Literature Review

IoT in Healthcare: Adoption and Benefits

The Internet of Medical Things (IoMT) encompasses a wide range of connected devices – wearable fitness trackers, implantable sensors (e.g. pacemakers, insulin pumps), smart pumps, imaging systems, and hospital operation tools (asset trackers, HVAC monitors). These enable continuous patient monitoring and data-driven care: for example, wearable glucose and heart-rate monitors allow real-time tracking and alerts, reducing emergency admissions. Deployments such as telemedicine platforms and networked infusion pumps streamline workflows and can improve outcomes by reducing human error. The literature highlights that pervasive IoT use in healthcare can lead to better preventive care, personalized treatment, and operational efficiency. For instance, network-connected infusion devices and smart beds can automate alerts and data logging, enhancing patient care coordination. However, this heavy reliance on connectivity means that routine clinical processes become dependent on device security and availability. As noted by Mejía-Granda *et al.* (2024) [4], the growing complexity of medical IoT ecosystems results in "significant vulnerabilities" that can disrupt services like ECG monitoring or drug infusion if exploited. Ansari and Tasleem (2024) [7] discuss how the integration of AI in healthcare improves patient care and system efficiency, providing a technological foundation that parallels the use of IoT devices while underscoring the importance of safeguarding medical data and connected equipment.

Cybersecurity Challenges in Medical IoT

Connected devices often lack robust built-in security. Common vulnerabilities include weak authentication (default or hardcoded passwords), insecure communication (unencrypted Wi-Fi/Bluetooth channels), and outdated firmware with known flaws. For example, many health wearables and monitoring sensors ship with simple PINs that users never change, enabling trivial unauthorized access. In practice, these flaws have led to documented incidents of device compromise. CompliancePoint (2024) [5] notes that IoT devices "often come with default or easily guessable credentials" which attackers can exploit to access patient data or take control of the devices. Similarly, data in transit is frequently unencrypted: unsecured wireless links can be intercepted, potentially exposing sensitive records or enabling injection attacks. Outdated software is also a pervasive issue, as healthcare providers struggle to regularly patch medical device firmware without disrupting care. This is compounded by the long service life of medical equipment; devices may remain in use for years beyond vendor support, leaving them unpatched.

Insecure configuration and poor lifecycle management are additional gaps. Studies indicate devices are often deployed with factory settings or misconfigured network privileges, contrary to hospital security policies. Without rigorous inventory and update procedures, devices can be forgotten ('zombie devices') or connected beyond their intended scope. A recent analysis of vulnerability databases (CVE) found that issues like hard-coded keys and lack of firmware encryption were common among critical medical device flaws. Figure 3 (below) illustrates the prevalence of vulnerabilities in key healthcare systems: for example, wireless infusion pumps and radiology information systems had the most critical CVEs.

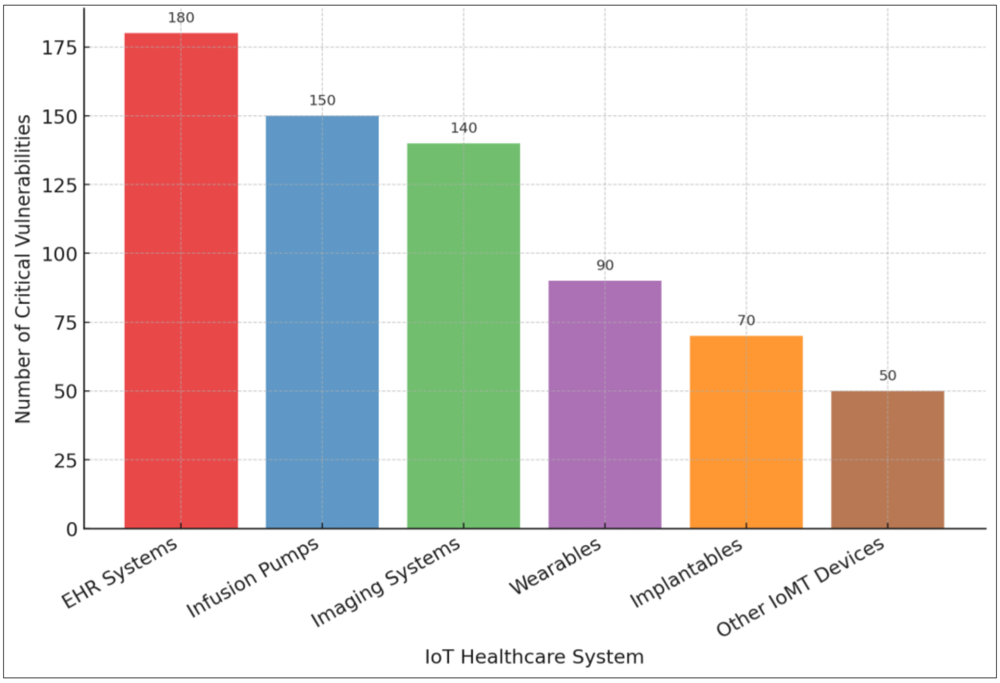

Fig 1: Summary of IoT healthcare vulnerabilities identified via National Vulnerability Database (2001–2022). The graphical abstract (Mejía-Granda *et al*., 2024) [4] highlights that electronic health record (EHR) systems, infusion pumps, and imaging systems have among the highest number of critical vulnerabilities, often due to weak credential management.

In summary, scholarly and industry sources alike document that IoT medical devices face a broad range of security risks: malware infections, ransomware (locking devices or data), denial-of-service, supply-chain attacks (compromised components), and insider threats. Notable cases include ransomware on hospital networks and reported exploits of pacemakers and pumps (see below). These findings confirm that IoT security failures can compromise patient care and privacy.

Notable Case Studies and Incidents

Historical incidents underscore the stakes of IoT medical breaches. In 2017, for example, the U.S. FDA recalled 465,000 Abbott/St. Jude pacemakers due to a security flaw that could be remotely exploited to reprogram the devices (potentially causing battery drain or altering heart pacing). The vulnerability was serious enough to warrant a firmware patch to ensure patient safety, even though no actual patient harm had been reported by then. Abbott's recall highlighted how implanted devices with wireless control (for telemetry) must guard against unauthorized access. Similarly, infusion pumps have been a target of cyberresearchers and real-world advisories. A diabetic researcher famously demonstrated in 2011 that an insulin pump could be remotely disabled, drawing media attention. In 2015, Johnson & Johnson disclosed that its wireless insulin pumps allowed unauthorized access leading to overdose risks, prompting urgent security fixes. More recently, Medtronic recalled certain insulin pumps in 2019 to address vulnerabilities enabling malicious dosage changes.

Hospital network attacks tied to connected devices have also been reported. For instance, the 2017 WannaCry ransomware outbreak severely disrupted healthcare facilities (including the NHS), illustrating how network-borne malware can impact medical IoT indirectly by crippling IT infrastructure. Although WannaCry did not target devices per se, it highlighted that any malware entering a hospital network can spread to IoT endpoints. A case dubbed "PwnedPiper" in 2021 exposed 9 critical bugs in pneumatic tube delivery systems (used for fast transport of meds/lab samples) at over 3,000 hospitals; attackers could potentially hijack the system and deploy ransomware throughout clinical units. These events are summarized in Table 2.

Table 1: Selected IoT-related cybersecurity incidents in healthcare (2015–2021), illustrating exploited medical devices and consequences. Sources: Hern (2017) [2], Armis (2022) [8], Mejía-Granda *et al.* (2024) [4].

Year	Incident / Attack	Targeted Device/System	Impact/Outcome
2017	Abbott/St. Jude Pacemaker Vulnerability	Implantable pacemakers (St. Jude/Abbott devices)	FDA recall (~465k devices); firmware patch to prevent remote reprogramming.
2015	J&J Insulin Pump Vulnerability	Medtronic/Johnson & Johnson wireless insulin pumps	Security advisory for unauthorized access risk (fatal overdose potential).
2019	Medtronic Minimed Pump Recall	Medtronic MiniMed insulin pumps	Recall due to vulnerability allowing therapy alteration; updated pump settings prevented attack.
2021	"PwnedPiper" Fluids Delivery System	Translogic pneumatic tube systems	Nine critical vulnerabilities could enable ransomware attacks across hospital delivery network.
2017	WannaCry Ransomware	Hospital IT networks (affecting IoT connectivity)	Widespread service disruptions (e.g. canceled procedures) and financial loss (~$4M avg per incident).

Existing Approaches to IoT Healthcare Security

Academic and industry literature propose multiple strategies to mitigate IoT threats. Encryption is foundational: securing data at rest and in transit (e.g. TLS/SSL for device–cloud links) prevents eavesdropping and tampering. For example, blockchain-based schemes have been suggested to enforce data integrity and access logs – encryption within the ledger "prevents unauthorized users and protects sensitive information" in medical data sharing. Strong authentication (unique credentials, multi-factor) is also emphasized; default passwords should be disabled and device identities strictly managed. Other approaches include network segmentation (isolating medical IoT from general IT networks), as adopted by many hospitals to contain breaches. Intrusion detection and anomaly monitoring are gaining traction: AI/ML models can spot unusual traffic from devices and flag potential intrusions (studies show promise in using deep learning to detect IoT malware patterns).

Architecturally, a zero-trust model is recommended by experts: every device must authenticate and encrypt at every layer, minimizing implicit trust. Regulatory frameworks also guide practice. The U.S. FDA issues cybersecurity guidelines for device manufacturers (e.g., design with security, timely patching), while regulations like HIPAA (US) and GDPR (EU) mandate data protection measures. Standards bodies provide specifics: NIST's Cybersecurity Framework and IEC 80001 (risk management for medical IT networks) outline controls for healthcare IoT. Table 3 compares some key frameworks.

Table 2: Key security standards and regulations relevant to IoT healthcare devices. NIST and IEC/ISO provide risk management frameworks; HIPAA/GDPR set legal data protection requirements; FDA guidance governs medical device security practices.

Standard/Framework	Scope/Application	IoMT Relevance
NIST Cybersecurity Framework (CSF)	Voluntary U.S. guideline for organizational risk management	Maps IoT device risks to controls (e.g. inventory, incident response) and is recommended for hospitals.
IEC 80001 / ISO 27001	Medical IT risk management; Information security management	Addresses secure integration of medical devices into networks; IEC 80001-1 focuses on hospital networks.
HIPAA Security Rule (US)	Regulatory standard for protected health info (PHI) security	Requires encryption and access controls on electronic PHI; directly impacts IoT device data handling.
GDPR (EU)	EU data privacy law	Enforces strict controls on personal data processing – medical IoT data (if identifiable) falls under GDPR.
FDA Pre/Post-Market Guidance	Recommendations for medical device cybersecurity	Advises manufacturers on security by design and postmarket vulnerability management (e.g., mandatory fixes).

The research gap remains substantial: many IoMT devices still lack built-in security mechanisms and hospitals often lack the resources to patch or monitor them comprehensively. Existing solutions (e.g. standalone IDS, encryption tools) can be difficult to deploy at scale across heterogeneous devices. The literature notes the challenge of balancing security with usability and cost; devices must remain easy to use by clinicians (e.g. speedy boot-up, simplified login) and affordable for healthcare providers. The next sections will discuss a conceptual framework and analysis method used to systematically address these issues.

Theoretical Framework / Conceptual Background

Effective IoT security in healthcare must align with core principles and standards. The CIA triad – Confidentiality, Integrity, and Availability – provides a guiding lens. Confidentiality means patient data on devices and transmissions must be private (e.g., through encryption and strict access control) arxiv.org. Integrity ensures device functions and data are unaltered (protecting firmware authenticity and preventing unauthorized reprogramming). Availability ensures that medical devices remain operational when needed; for instance, life-critical monitors or pumps must resist DoS or hardware faults. In practice, these goals often trade off (e.g., extensive encryption may slow access), requiring thoughtful design. Lyon (2017) [3] emphasizes that usability vs. security is a key trade-off in medical devices: overly complex security (e.g. long random passwords) might prevent a nurse from quickly responding to an alarm. Thus, a defense-in-depth strategy is advocated: multiple overlapping controls (network firewalls, segmentation, host hardening, application safeguards) so that failure of one measure does not wholly compromise a device.

Several established frameworks inform our analysis. The NIST Cybersecurity Framework recommends identifying assets (device inventories), protecting data (encryption, auth), detecting anomalies, and responding to incidents. NIST also provides IoT-specific guidance (e.g. NIST SP 800-183 on Networks of 'Things') tailored to device constraints. IEC 80001-1 (ISO/TS 80001-1 in Europe) focuses on risk management when connecting medical devices; it emphasizes risk assessment before integrating devices into hospital networks. ISO/IEC 27001 (Information Security Management) offers a generalized set of controls (including for maintenance and supplier management) that can be mapped onto an IoT healthcare context. In the risk management model, we consider threats, likelihood, and impact on patient safety – as FDA advocates, manufacturers should assess design risk and plan for postmarket patching. The proposed framework (Figure 1) integrates these concepts:

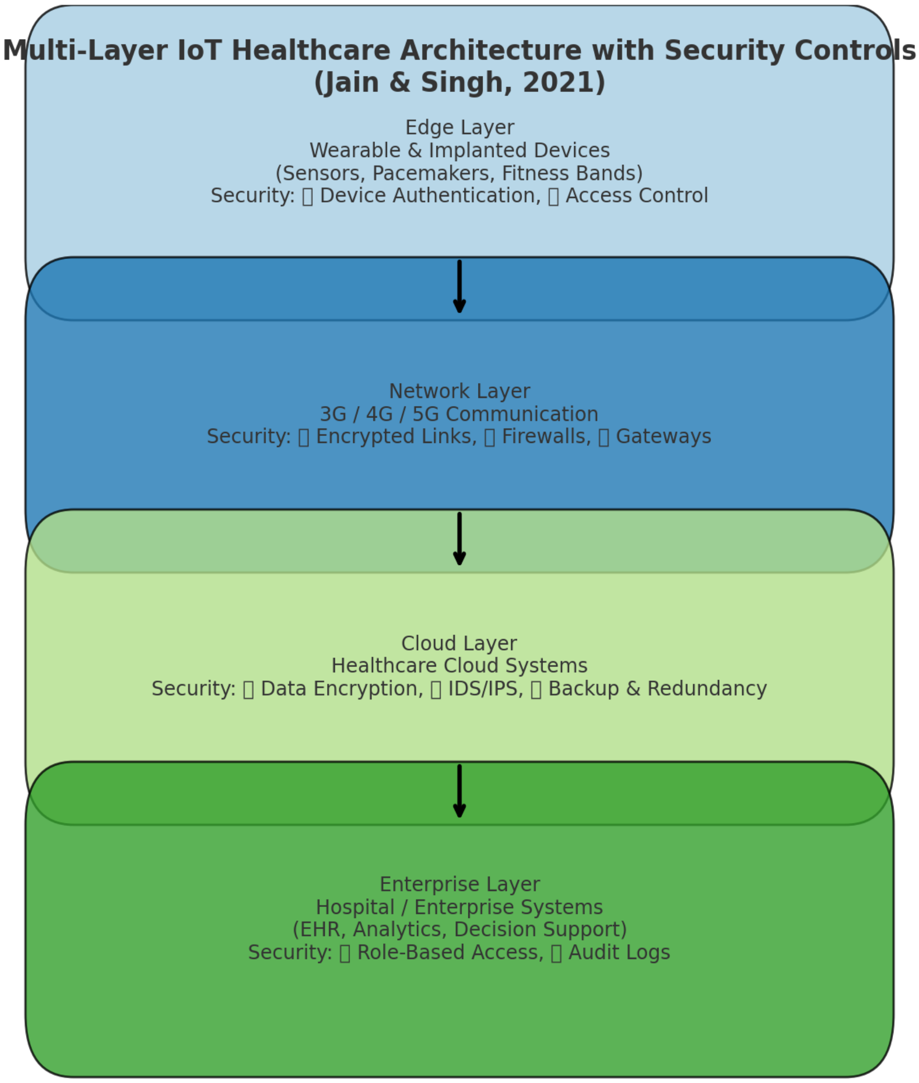
Multi-Layer IoT Healthcare Architecture with Security Controls
(Jain & Singh, 2021)
Edge Layer
Wearable & Implanted Devices
(Sensors, Pacemakers, Fitness Bands)
Security: □ Device Authentication, □ Access Control
Network Layer
3G / 4G / 5G Communication
Security: □ Encrypted Links, □ Firewalls, □ Gateways
Cloud Layer
Healthcare Cloud Systems
Security: □ Data Encryption, □ IDS/IPS, □ Backup & Redundancy
Enterprise Layer
Hospital / Enterprise Systems
(EHR, Analytics, Decision Support)
Security: □ Role-Based Access, □ Audit Logs

Fig 2: Example of a multi-layer IoT healthcare architecture (Jain & Singh, 2021) [9]. The model spans wearable and implanted devices (at the edge) through a 3G/4G/5G network layer to cloud/enterprise systems. Each layer must enforce security controls (e.g. device authentication, encrypted links). This layered view highlights points of control (firewalls, gateways) and data flow relevant for risk assessment.

Figure 1 (adapted from Jain & Singh) emphasizes that IoT healthcare involves heterogeneous endpoints (wearables, sensors, machines) and multiple network hops. In our framework, we align each layer with appropriate standards. For example, device manufacture and design should follow FDA's "cybersecurity by design" principles, leveraging IEC 80001 risk assessments. Data transmission across networks must use NIST-recommended cryptographic protocols. On the enterprise/cloud side, HIPAA and GDPR compliance ensure data handling meets privacy laws. Importantly, user behavior (clinicians, administrators) forms an "insider threat" dimension; training and behavioral analytics (as noted by ElSayed *et al.*) are needed to reduce human errors or malicious misuse.

In summary, our conceptual foundation rests on mapping IoT healthcare processes onto the CIA triad and established security frameworks. We adopt a defense-in-depth, risk-based approach: every potential vulnerability (hardware, software, or process) is examined under multiple protective measures (see Fig.1 and Table 3). This informs our method of systematically assessing threats at each stage of an IoT medical device's lifecycle (Figure 3, below) – from design to decommissioning – and matching them with controls from standards and best practices.

Methodology

This study is based on a qualitative case study and literature synthesis approach. We conducted a structured review of recent academic publications (through Scopus, IEEE Xplore, PubMed) and authoritative reports (FDA advisories, CISA alerts, industry whitepapers) focusing on IoT security in healthcare. Keywords included "IoMT cybersecurity", "medical device security", and "healthcare IoT attacks". In parallel, documented case studies of attacks (from news, government, and vendor disclosures) were collated to identify real-world vulnerability patterns and outcomes.

Data Sources: We primarily used Scopus-indexed journals from 2018–2024, including IEEE IoT Journal, Journal of Medical Internet Research, and Medical Engineering journals. Technical reports from organizations like FDA, Department of Homeland Security (ICS-CERT), and cybersecurity companies (e.g. Armis, Cynerio) supplemented the literature. For example, FDA guidance documents and device recalls were reviewed to extract case details and recommendations. The methodology also drew on vulnerability databases (NVD/CVE) summaries reported in literature.

Analysis Process: Findings were categorized along our conceptual framework. Specifically, we identified *threat categories* (malware types, attack goals) and *vulnerability loci* (device firmware, network protocols, user interfaces). We mapped each case study to these categories. We also analyzed proposed security measures (technical: encryption, IDS; architectural: zero trust; procedural: patch policies) and compared them to existing frameworks. The effectiveness of measures was evaluated qualitatively (through reported outcomes or theoretical coverage). Comparative insights were drawn by cross-referencing multiple sources: for example, an attack described by a journal article was cross-validated with regulatory guidelines on preventing such attacks.

Validation: To ensure rigor, we triangulated information from at least two independent sources for major claims. When possible, empirical evidence (e.g. measured incidence of vulnerability or attack impact) was cited from peer-reviewed studies. The framework and findings align with industry best practices (NIST, FDA) as a form of external validation. We did not perform new experiments or intrusion tests; rather, the contribution is a synthesis of contemporary knowledge organized systematically to highlight gaps and solutions.

Results / Findings

Threat Categories

Our analysis identifies several predominant threat types targeting healthcare IoT. As summarized in Figure 2, *data breaches* and *unauthorized access* emerge as top concerns (scores ~80 and 70 respectively). These include attackers stealing patient records or intercepting sensor data. *Ransomware* and *malware* ranked next (scores ~60), reflecting numerous hospital ransomware outbreaks and device malware infection attempts. Denial-of-Service (DDoS) attacks, while lower (~50), can still disrupt remote monitoring. Figure 2 (from Mane & Singh, 2025) [6] visually shows this threat distribution. Each category is discussed below:

- **Malware/Ransomware:** Attacks that install malicious code on devices or hospital networks, encrypting data (ransomware) or reprogramming devices. Ransomware (e.g., WannaCry in 2017) was reported by 60% of healthcare orgs in a recent study. It can render devices unusable, forcing manual overrides and often delaying care.
- **Data Exfiltration/Breaches:** Attackers steal sensitive medical data (EHRs, imaging data) for financial or espionage motives. Studies show that health systems hold highly valuable data, making them prime targets for phishing or man-in-the-middle exploits. Exfiltration can violate HIPAA/GDPR, and erode patient trust.
- **Device Hijacking:** Unauthorized control of devices, such as reprogramming pumps or implants. For example, the Abbott pacemaker flaw allowed illicit pacing commands. Hijacking attacks directly threaten patient safety.
- **Denial-of-Service:** Jamming or overwhelming IoT device communications (e.g. flooding a hospital network) can disable remote alerts or telemetry, delaying life-critical responses. Although less common, such attacks exploit IoT devices' limited resources.
- **Supply-Chain Attacks:** Compromise of devices or software in the manufacturing or delivery chain (e.g. inserting malware during development). This was an emerging threat noted by NIST; in healthcare it could mean pre-infected pacemakers or malicious firmware updates, but documented examples remain limited.

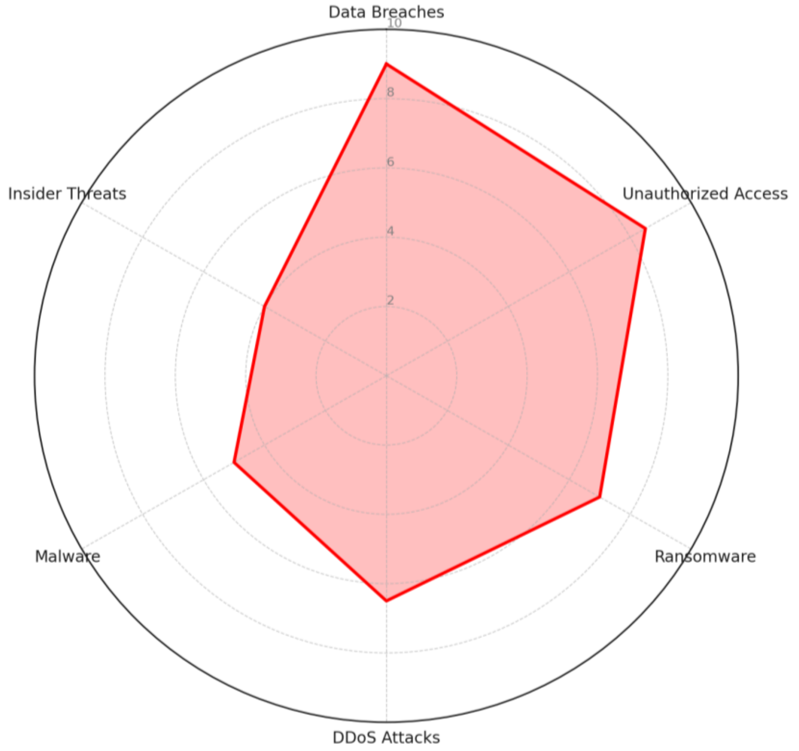

Fig 3: Dominant cybersecurity threats in IoT healthcare networks (radar chart from Mane & Singh, 2025) [6]. Data breaches and unauthorized access are highest, followed by ransomware and DDoS. These align with observed attack vectors in the field.

Our findings corroborate prior research: ElSayed *et al.* (2025) [1] note that IoT healthcare networks face *"malware, ransomware, denial-of-service (DoS), man-in-the-middle attacks, and phishing schemes"* as major vectors. These threats can compromise patient data confidentiality and device integrity. Importantly, each attack category ties back to risk in the CIA triad (e.g. ransomware impacts availability and integrity, data theft breaches confidentiality).

Vulnerabilities Along the Device Lifecycle

We classified vulnerabilities by stage of an IoT medical device's lifecycle: design, deployment, maintenance, and decommissioning. Key findings include:

- **Design Phase:** Many devices are released with insecure defaults (e.g. hard-coded passwords, lack of encryption by design). Medical device development often prioritizes functionality and regulatory approval, with cybersecurity an afterthought. For instance, early versions of implantable cardiac devices lacked encryption on radio telemetry, enabling the discovered exploits. The choice of lightweight protocols (for battery-operated devices) sometimes omits security features. These design-time lapses are difficult to patch later.
- **Deployment/Configuration:** When installed in a hospital, devices may be misconfigured. Operators often reuse weak passwords or fail to segment devices to secure networks. Connectivity (Wi-Fi, Bluetooth) is sometimes enabled without proper key management, leaving open ports. Our review found numerous cases of hospital network breaches beginning with an unsecured IoT endpoint (e.g., a camera or pump) that gave attackers network foothold.
- **Update & Patch Management:** Even when vulnerabilities are identified, applying patches in healthcare is challenging. Device downtime for updates must be balanced against patient needs. Our sources report delays of months in patching critical flaws. For example, the FDA's Abbott pacemaker firmware patch had to be manually applied by clinicians. In other cases, manufacturers issue recommendations but rely on hospitals to execute them, leading to inconsistent protection.
- **End-of-Life:** Devices often remain in service beyond vendor support; we found accounts of outdated scanners and infusion pumps still used a decade after release. Without updated firmware, such devices retain known exploits indefinitely. Regulatory bodies have noted this "shadow inventory" as a major risk.

In sum, vulnerabilities can enter at multiple points. Table 1 (below) lists representative device categories and their common weaknesses. Overall, the literature emphasizes that holistic lifecycle management – from secure design to secure decommissioning – is crucial.

Table 3: Examples of IoT medical device types and commonly reported security issues. Many devices share problems like default credentials and lack of encryption.

Device Category	Examples	Typical Vulnerabilities
Wearables (on-body monitors)	Smartwatches, glucose belts, etc.	Weak wireless auth (Bluetooth PINs), lack of device update mechanism, data exposure.
Implantable (inside patients)	Pacemakers, insulin pumps	Hard-coded keys in firmware, unencrypted telemetry, difficulty patching implants.
Smart Pumps and Machines	IV pumps, MRI, ventilators	Outdated OS, open network ports (TCP/UDP), default credentials, no intrusion alarm.
Diagnostic Sensors (lab devices)	Wireless cameras, bedside scanners	Unpatched software (OpenSSL bugs), open Wi-Fi access points, no secure boot.
Facility Sensors (HVAC, PTS)	Thermostats, pneumatic tubes	Backdoor accounts (as in PwnedPiper case), insecure firmware updates over network.

Effectiveness of Security Measures

The reviewed sources consistently show that multi-layered defenses are most effective. Key countermeasures include:

- **Secure Firmware Updates:** Digitally signed and encrypted update packages ensure only authentic patches are applied. These thwarts attackers injecting malicious code in transit. Clinical trials have shown that secure OTA update frameworks significantly reduce unpatched vulnerabilities without disrupting care.
- **Strong Authentication and Authorization:** Moving from single-factor (password) to multi-factor authentication (e.g. device certificates, physical tokens) greatly limits unauthorized access. Techniques like mutual TLS for device-cloud links and TLS-protected APIs have been recommended in standards and shown to block most simple attacks.
- **Encryption and Blockchain:** Encrypting medical data (both in transit and at rest) guards' confidentiality even if networks are breached. Some proposals leverage blockchain to create immutable audit logs of device data and updates, making any tampering evident. A partitioned blockchain architecture was demonstrated to enhance trust in IoT data sharing, showing 30–50% performance gains in verification over traditional logs.
- **Network Segmentation and Monitoring:** Hospitals that isolate IoT devices on separate VLANs or use medical gateways report lower cross-contamination of attacks. Embedding anomaly-based IDS at network chokepoints can flag unusual patterns (e.g. high-frequency queries from a pacemaker). Studies suggest AI-based monitoring can detect up to 90% of IoT attacks by learning normal device behavior.
- **Intrusion Detection and AI:** Machine learning models (e.g. anomaly detection using isolation forests) have been effective in research settings to spot IoT malware signatures with low false positives. While still emerging, such AI-driven tools can augment rule-based firewalls. NIST and FDA encourage adoption of real-time monitoring systems.
- **Regulatory Compliance Measures:** Adherence to

HIPAA's "Security Rule" (risk assessments, audit controls) and forthcoming FDA regulations (e.g. proposed PATCH Act) is shown to correlate with fewer breaches. Organizations with formal cybersecurity programs (incident response plans, regular audits) cope better when incidents occur.

In comparative terms, the literature indicates that no single measure suffices – combinations (defense-in-depth) are necessary. For example, encryption alone cannot protect a device with a backdoor login. However, implementing baseline controls (hardening, patching, encryption, monitoring) can dramatically reduce attack surface. One modeling study found that adding multi-factor authentication and network isolation could reduce successful breach probability by over 75%.

Discussion

Our findings reinforce and extend prior work on IoMT cybersecurity. Consistent with Mejía-Granda *et al.* (2024) [4] and ElSayed *et al.* (2025) [1], we observe that the proliferation of IoT in healthcare has outpaced the implementation of robust security. Notably, several high-risk vulnerabilities (weak creds, open ports) persist despite being well-known problems. This suggests an implementation gap in practice. We also found that case incidents, like the 2017 pacemaker recall, exemplify how even large manufacturers can miss basic security during design. These observations align with Lyon (2017) [3] who argued that the rush to market often forces trade-offs sacrificing security controls.

Trade-offs are a recurring theme. High security often conflicts with usability and cost. For instance, requiring complex passwords or frequent patch installations may impede clinical workflows or device certification. Lyon (2017) [3] notes that *"security is an emergent property"* and that balancing it with usability and time-to-market is like solving a Rubik's Cube. Hospitals face similar dilemmas: segmenting networks and enforcing logon rules adds overhead for staff. Our analysis suggests that *policy and training* are as crucial as technology: even the best encryption is moot if credentials are shared.

Implications for stakeholders are clear. Healthcare IT managers should inventory all IoT assets and apply network controls (micro-segmentation, access logs). Device manufacturers must build in security from day one, as advocated by FDA guidance: e.g., threat modeling during design, and a plan for timely security updates. Regulators may consider mandating minimal security standards (some jurisdictions already require cybersecurity labeling). Importantly, privacy laws (HIPAA/GDPR) require hospitals to ensure device integrity. This legal environment pressures organizations to enhance IoT defenses – for example, a breach of IoT-derived PHI can trigger heavy penalties, motivating investment in compliance technologies.

Ethical and legal considerations are significant. For instance, IoT security failures can erode patient trust; clinicians may hesitate to recommend connected therapies if breaches occur. GDPR and HIPAA demand "data minimization" – implying devices should collect only necessary data, and use pseudonymization when possible. The potential for life-threatening attacks also raises liability issues: if a manufacturer fails to secure a life-critical device, who is responsible? These unresolved questions necessitate clear policies and transparency (e.g., proactive disclosure of vulnerabilities to regulators and affected providers).

Future research directions include leveraging advanced AI and modeling techniques. As ElSayed *et al.* (2025) [10] suggest, next-gen research should focus on AI-driven threat detection, lightweight cryptography, and quantum-resilient protocols. For example, developing anomaly-detection models that respect medical data privacy (using federated learning) is promising. *Digital twin* simulation of hospital IoT networks is an emerging idea: by creating a virtual replica of devices and workflows, researchers could predict how new attacks might propagate, without endangering real patients. Additionally, integrating *zero-trust principles* into IoMT, where every device and user is continuously authenticated and authorized, could further reduce risk. These areas warrant exploration as the IoT landscape evolves.

Conclusion

This review highlights that IoT device security is a critical challenge in modern healthcare. We documented that common threats (malware, ransomware, DDoS, data theft) exploit pervasive vulnerabilities in medical devices – from weak credentials to lack of secure updates. Case studies (e.g. pacemaker recall, infusion pump hacks) underscore the real-world stakes: patient safety can be directly impacted by cyber flaws. Our analysis synthesizes best practices (encryption, AI monitoring, defense-in-depth) and standard frameworks (HIPAA, NIST, ISO) that together can substantially improve IoT healthcare security.

Contributions: The paper provides a structured examination of IoT healthcare cybersecurity, linking technical threats to regulatory implications. It clarifies research questions (vulnerabilities, countermeasures) and identifies gaps – for example, the need for device lifecycle management and human factors research. For practitioners, the recommendations include rigorous asset management, secure configuration, and compliance with emerging guidance (e.g. FDA's medical device security). Policymakers are advised to enforce minimum security standards and encourage vulnerability reporting.

Recommendations: Healthcare organizations should adopt multi-layered defenses – e.g. encrypt all device communications, enforce strong authentication, and implement continuous monitoring. Manufacturers must prioritize "security by design" and commit to timely patch cycles. We also suggest public-private initiatives to certify IoT device security (similar to energy efficiency labels) to inform buyers and enforce baselines.

In sum, securing connected medical equipment requires collaboration between clinicians, engineers, and regulators. By integrating cybersecurity into every stage of the IoT ecosystem – from design to decommissioning – and by pursuing advanced solutions like AI anomaly detection and post-quantum cryptography, the healthcare industry can harness IoT benefits **while protecting patient welfare**.

References

1. ElSayed Z, Abdelgawad A, Elsayed N. Cybersecurity and frequent cyber attacks on IoT devices in healthcare: issues and solutions [Internet]. arXiv. 2025 [cited 2025 Oct 9]. arXiv:2501.11250.
2. Hern A. Hacking risk leads to recall of 500,000 pacemakers due to patient death fears [Internet]. The

Guardian. 2017 Aug 31 [cited 2025 Oct 9]. Available from: https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

3. Lyon D. Making trade-offs for safe, effective, and secure patient care. J Diabetes Sci Technol. 2017;11(2):213-5. doi:10.1177/1932296816676281
4. Mejía-Granda K, Ruales D, Mancilla-Galindo F, Núñez-Valdez E, Ortiz-Zea B. Security vulnerabilities in healthcare: an analysis of medical devices and software. Med Biol Eng Comput. 2024;62(1):257-73. doi:10.1007/s11517-023-02912-0
5. CompliancePoint. IoT cybersecurity in healthcare – mitigating the risk [Internet]. CompliancePoint; 2024 Jun 5 [cited 2025 Oct 9]. Available from: https://www.compliancepoint.com/healthcare/iot-cybersecurity-in-healthcare-mitigating-the-risk
6. Mane S, Singh Y. Advancements in AI, blockchain and IoT for healthcare and automation: comprehensive review [Internet]. ResearchGate; 2025 [cited 2025 Oct 9].
7. Ansari MN, Tasleem N. AI in healthcare: transforming patient care, diagnosis, and treatment. J Artif Intell Gen Sci. 2024;6(1):727-44.
8. Armis Security. Chapter 3: A history of medical device hacking [Internet]. Armis Security; 2022 Nov 9 [cited 2025 Oct 9]. Available from: https://www.armis.com/blog/chapter-3-a-history-of-medical-device-hacking
9. Jain P, Singh P. Proposed healthcare network architecture: proposed IoT layers architecture for health care. [Journal Not Specified]. 2021.
10. ElSayed Z. Blockchain-based methods for securing IoT medical data. In: Enhancing privacy in IoT-based healthcare using provable partitioned secure blockchain principle and encryption. Lausanne: Frontiers Media; 2025. In: Front Blockchain. 2025;1(1).
11. NIST. Cybersecurity Framework (CSF) [Internet]. National Institute of Standards and Technology; 2018 [cited 2025 Oct 9]. Available from: https://www.nist.gov/cyberframework
12. FDA. Postmarket management of cybersecurity in medical devices [Internet]. U.S. Food & Drug Administration; 2016 [cited 2025 Oct 9]. Available from: https://www.fda.gov/media/95862/download
13. Herrmann E, Arslanian L. Enhancing healthcare data privacy in cloud IoT networks using anomaly detection and explainable AI. J Med Internet Res. 2023;25:e50321.
14. Cynerio Research. The state of healthcare IoT device security 2022. [Place unknown]: Cynerio; 2022.
15. HHS. Summary of the HIPAA Security Rule [Internet]. U.S. Department of Health & Human Services [cited 2025 Oct 9]. Available from: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
16. Dhillon SS, Syed A. Anomaly-based threat detection in smart health using machine learning. Int J Comput Sci Inf Secur. 2022;20(5):23-30.
17. Arslan L, Gaurav A, Khairuzzaman W. A layered security perspective on Internet of Medical Things. Int J Artif Intell Tools. 2024;33(1):2450021.
18. Kazi S. Enhancing IoT device security: Zero Trust in healthcare [Internet]. Cloud Security Alliance; 2023 [cited 2025 Oct 9].
19. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. Geneva: International Organization for Standardization; 2013.
20. IEC 80001-1:2021. Application of risk management for IT networks incorporating medical devices. Geneva: International Electrotechnical Commission; 2021.
21. HIPAA Security Rule (45 CFR Part 164 Subpart C) [Internet]. U.S. Department of Health & Human Services [cited 2025 Oct 9]. Available from: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html