Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 22 No. 7 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v22i07.60469

PAPER

Cybersecurity Maturity and Risk Profiling of AI-Enabled Medical Sensors: A Cross-Manufacturer Comparative Analysis

Filip Tsvetanov (✉)

South-West University, Blagoevgrad, Bulgaria

ftsvetanov@swu.bg

ABSTRACT

The rapid integration of artificial intelligence (AI) into modern medical sensors—from multi-parameter hospital patches to ambulatory wearables, implantable cardiac devices, and continuous glucose monitoring (CGM)—is transforming clinical diagnostics and patient monitoring. Still, it introduces complex cybersecurity risks spanning device firmware, wireless communication, cloud infrastructure, and AI models. This study proposes a new integrated methodology for assessing cybersecurity maturity in AI-enhanced medical sensors based on ISO 14971, NIST 800-30/53, and AHP weighting. Using ten key criteria, it enables objective comparison among leading manufacturers and generates two indicators: a weighted security score (WSS) and a risk profile score (RPS). The study reveals critical vulnerabilities in the communication security and AI modules of specific devices, and greater cryptographic resilience in implantable systems. The results have direct practical value for engineers, clinicians, and organizations that implement such devices, as well as for educating students in medical technology and cybersecurity. The publication also highlights the need to develop unified AI-oriented security standards throughout the life cycle of medical sensor devices.

KEYWORDS

artificial intelligence (AI)-enabled medical sensors, cybersecurity maturity, risk profiling, implantable medical devices, multi-criteria security evaluation

1 INTRODUCTION

In recent years, the integration of artificial intelligence (AI) into medical sensors and Internet of Medical Things (IoMT) devices has revolutionized healthcare, enabling more precise monitoring, early diagnosis, and personalized therapy. This digital transformation has also significantly increased the opportunities for cyberattacks, as connected medical devices are vulnerable due to limited resources,

Tsvetanov, F. (2026). Cybersecurity Maturity and Risk Profiling of AI-Enabled Medical Sensors: A Cross-Manufacturer Comparative Analysis. *International Journal of Online and Biomedical Engineering (iJOE)*, 22(7), pp. 4–25. https://doi.org/10.3991/ijoe.v22i07.60469

Article submitted 2026-01-06. Revision uploaded 2026-02-14. Final acceptance 2026-02-19.

heterogeneous communication protocols, and insufficient authentication and security mechanisms [1], [2], [3]. Medical sensors have become essential components of modern healthcare, enabling continuous monitoring of physiological parameters such as ECG, SpO_2, respiratory rate, glucose concentration, and motor activity. The evolution towards the implementation of improved sensors through various AI tools and technologies in healthcare is leading to an increase in the amount of data generated and collected, the creation of better algorithms for diagnosis and management, but also to an increase in the complexity of sensors [4], making cybersecurity not just a technical requirement, but an imperative for clinical safety. In addition, the increasing volume of sensitive medical data collected, transmitted, and processed in real time requires the implementation of advanced cybersecurity mechanisms to ensure the confidentiality, integrity, and availability of information [5]. AI is emerging as a key tool to enhance cybersecurity in IoMT, enabling automated anomaly detection, intelligent threat response, and dynamic adaptation to emerging attacks [6]. Modern AI-based intrusion detection systems (IDSs) and their integration with technologies such as blockchain, federated learning, and homomorphic encryption significantly enhance the protection of medical sensors [7], [8]. It should be noted that the industry is now well-positioned to implement secure communication protocols in these devices, such as AES, TLS, and secure BLE. At the same time, there is a lack of a unified framework for protecting AI models and insufficient protection against hostile machine learning (ML). The problem is exacerbated when devices are used in non-clinical environments (home monitoring), where the risks increase significantly. Existing approaches to cybersecurity risk assessment for AI-based medical devices are largely based on regulatory and risk-based frameworks that include cybersecurity as part of the overall safety and lifecycle management of devices [9]. While these frameworks provide basic guidance for compliance and post-market monitoring, they are often challenged by the dynamic, adaptive nature of AI-based medical software, whose risk profiles can evolve over time through continuous training, data updates, and software modifications [10]. To address these limitations, recent research has explored AI-based techniques for cybersecurity risk analysis and threat detection in IoMT environments, with a particular focus on anomaly detection and real-time monitoring of medical sensors and connected devices [11]. System-level frameworks have also been proposed to improve AI-based cybersecurity by combining risk prediction, continuous monitoring, and compliance assessment mechanisms to improve the overall resilience of the system [12]. At the same time, review studies [13], [14] highlight that existing methods mainly assess cybersecurity risks at the level of individual devices, network behavior, or regulatory compliance, and often do not sufficiently address AI-specific threats, such as data poisoning, model manipulation, and training data compromise. However, there are significant differences in cybersecurity approaches and effectiveness among leading vendors, which necessitate a systematic comparative analysis of the mechanisms, architectures, and standards used [8], [10].

The authors in [15] conduct a study on risk assessment and management for IoMT and related issues. They emphasize that cybersecurity risks are difficult to assess, especially quantitatively, due to the unpredictable nature of vulnerabilities, the current state of research, and the underexplored area of risk assessment and management for IoMT. In summary, they state that there is a research gap in risk management and security assessment for information systems in environments that include IoMT devices.

In this context, the work proposes a multi-criteria methodology for assessing cybersecurity maturity in AI-based medical sensor ecosystems, enabling systematic comparisons between manufacturers and risk profiling. Such an approach would support the identification of best practices and existing gaps, thus contributing to the development of secure and resilient AI-based medical IoT systems.

2 PRIMARY CYBER THREATS AND VULNERABILITIES FACING MEDICAL SENSORS WITH AI-ENHANCED

The problem of cyber threats and vulnerabilities in medical sensors is extremely relevant and has attracted increased interest from the academic community. These dangers are also determined by the system architecture of AI-enhanced medical sensors, shown in Figure 1.

The main threats include denial-of-service (DoS) attacks, false data injection (FDIA), unauthorized access, eavesdropping, malware, and data manipulation during transmission [16, 17, 18, 19, 20]. Vulnerabilities arise from limited device resources, heterogeneous communication protocols, a lack of standardized authentication and encryption mechanisms, and the difficulty of implementing traditional real-time security measures [3]. The main threats and vulnerabilities of AI-enabled medical sensors are summarized in Figure 2.

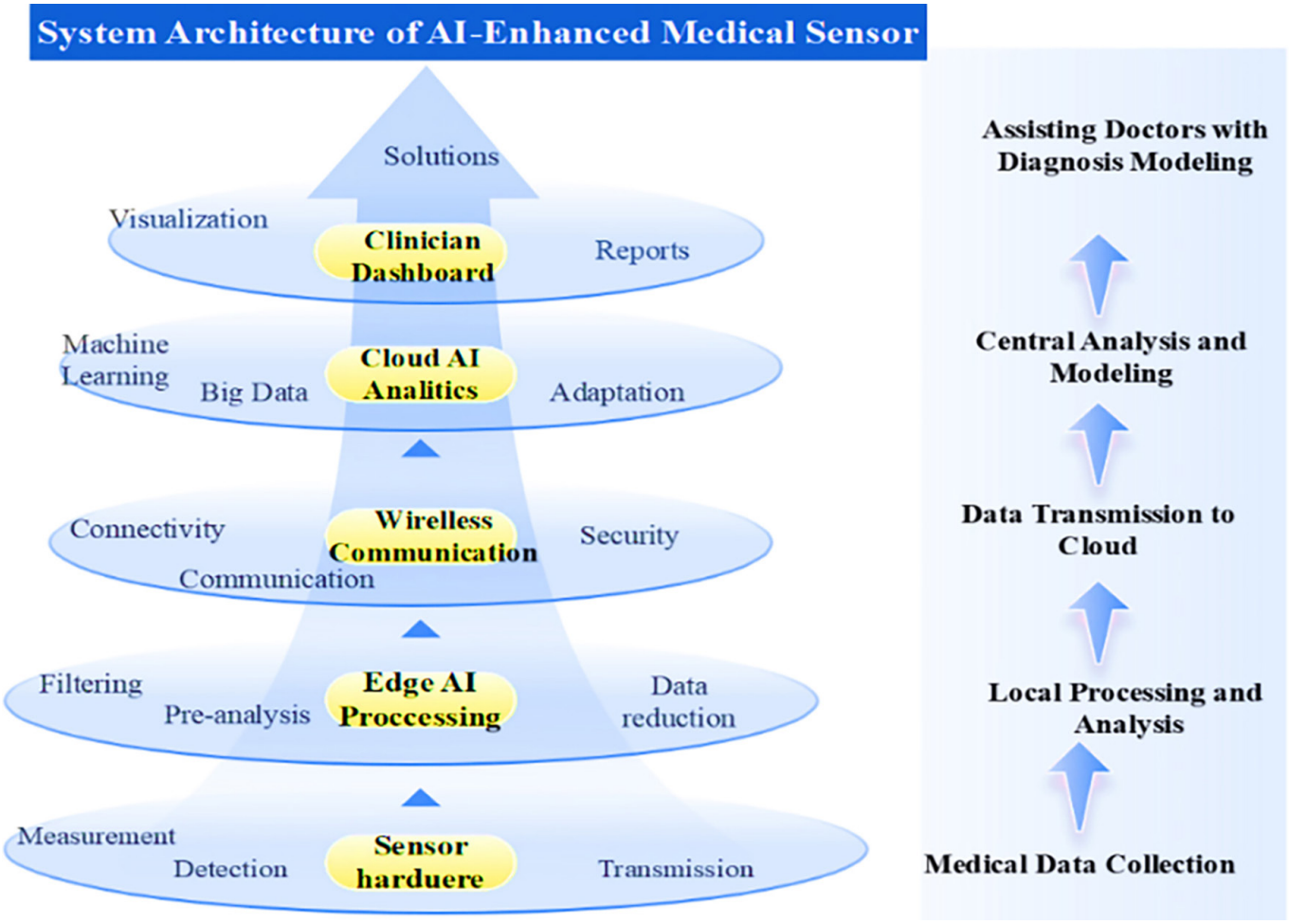

Fig. 1. System architecture of medical sensors with AI-enhanced

Fig. 2. Key cyber threats and vulnerabilities in medical sensors with AI-enhanced

2.1 Communication layer (BLE/Wi-Fi/LTE, telemetry)

Medical sensors commonly use BLE, but the protocol includes significant vulnerabilities. Weaknesses in the pairing process may expose the secret key and allow unauthorized device access [21]. Additional risks arise from short encryption keys, lack of user authentication, and susceptibility to MiTM, Replay, and device-cloning attacks, which can compromise patient data [22]. Poor cryptographic practices and battery-drain attacks further degrade system reliability. SoC vulnerabilities affect both software and the underlying hardware architecture [23]. Excessive or malformed BLE traffic can cause crashes or rapid battery depletion. At the same time, flaws in SDKs or firmware enable remote exploitation, including DoS attacks, code injection, whole device takeover, and unauthorized access to sensitive data [23, 24].

2.2 Firmware or hardware security layer

This layer is critical because it establishes trust in the device itself before it can transmit data, perform AI inference, or initiate communication. A compromised *bootloader* or *firmware* means that all higher-level protections become meaningless. These threats include: Unauthorized Firmware Update, Firmware Downgrade/ Rollback Attack, Hardware-level cryptographic key extraction Attacks, and Physical Tampering [3, 25, 26].

2.3 Cloud or infrastructure layer (SaMD or AI-cloud)

This layer, which serves SaMD (software as a medical device) and AI analytics platforms, is critical for the security of medical sensors. The main threats and vulnerabilities of this layer include: weak authentication/authorization [27], Inadequate Token/Key Management [28], Unsecured FHIR/HL7 APIs, and Supply Chain vulnerabilities. Overcoming these vulnerabilities includes building a zero-trust architecture; implementing RBAC/ABAC systems; centralizing secret management; network segmentation; separating cloud devices/sensors that send data to core clinical systems; and using VLANs, firewalls, IDS/IPS, continuous monitoring, and logging.

2.4 Artificial intelligence-specific layer for security threats

The AI layer in medical sensors introduces unique risks because it processes sensor data directly. Here, attacks target not only software bugs but also the AI model's mathematical structure or the data distribution itself, resulting in distorted sensor outputs and threats to model integrity and intellectual property. Key attack categories include Adversarial Attacks [29], Data Poisoning during model training [30], Model Extraction or Inversion attacks compromising confidentiality [31], Runtime Attacks that manipulate or disable model computations, and Model Drift, which degrades safety if uncontrolled [32]. Ensuring medical safety requires AI-specific countermeasures, as shown in Figure 3.

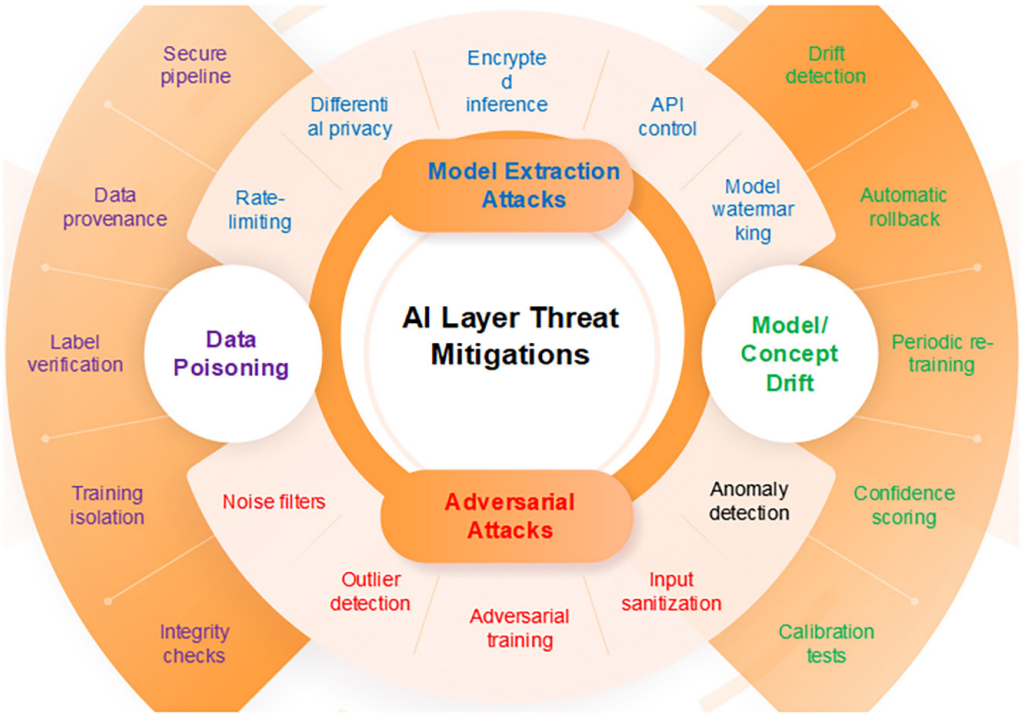

Fig. 3. Countermeasures to address AI threats in medical sensors

2.5 Implantable devices (ICM, CRT, ICD, stimulators)

Implantable medical devices (IMDs)—including ICMs, pacemakers, ICDs, CRT devices, and neurostimulators—represent the most safety-critical class of medical systems. Their cyber risk is heightened by long life cycles, limited hardware resources, constrained communication channels, and the possibility of remote configuration [33]. Key threats include: insecure communication interfaces [33]; vulnerabilities in remote/OTA configuration and in the implant–home hub link, often the weakest point in the ecosystem [34, 35]; outdated algorithms and non-upgradable hardware due to long device lifetimes; and physical attacks or reverse engineering with low likelihood but high impact [36]. Home-monitoring units and gateways also pose significant vulnerabilities [35], [38]. Countermeasures (see Figure 4) are essential to meet the requirements of FDA Premarket Guidance 2023–2025 [36] and IEC 81001-5-1 [37].

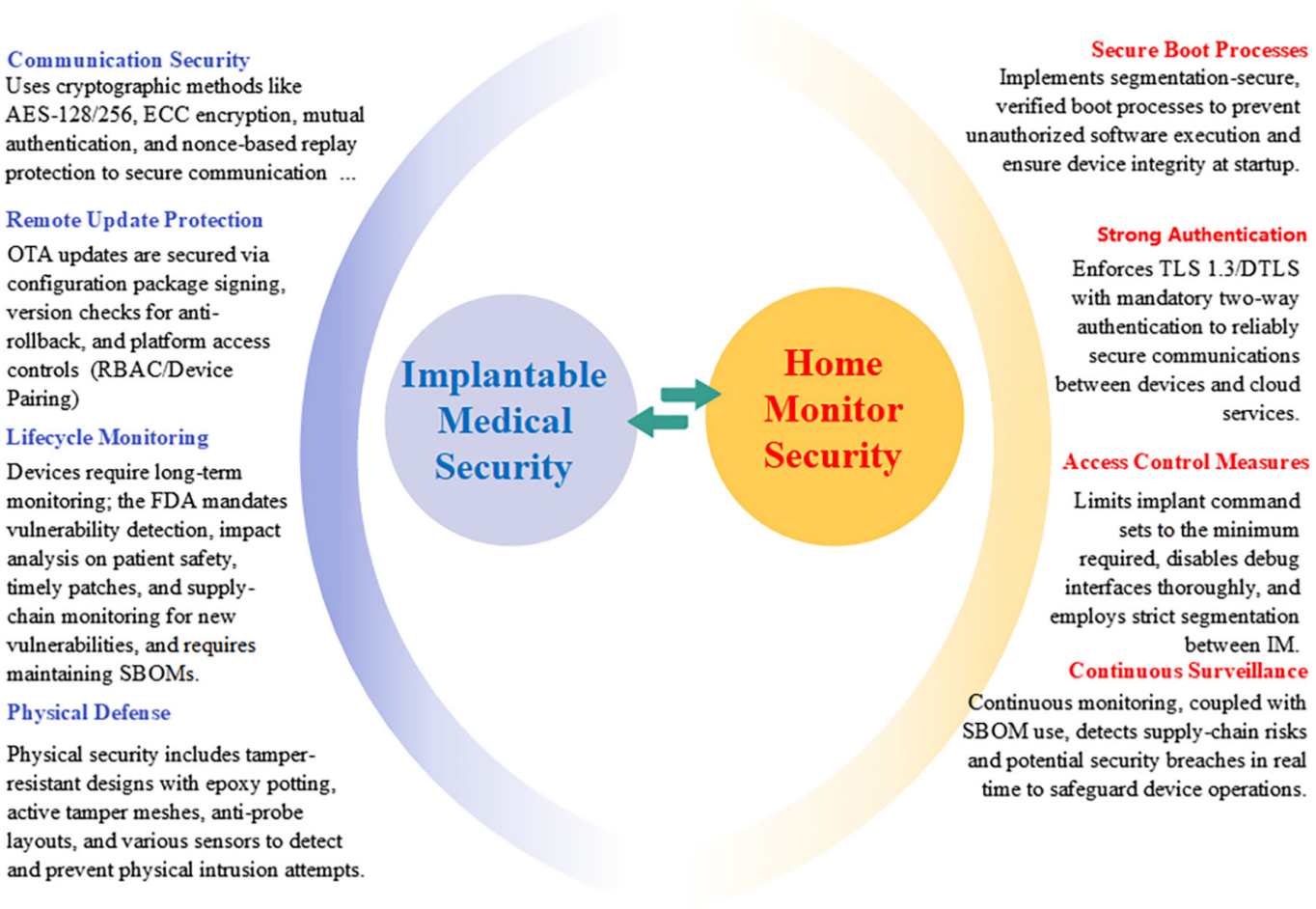

Fig. 4. Countermeasures to address security threats to implantable medical devices

2.6 Hospital platforms or getaways, home monitor

Home-monitor and gateway devices are the weakest link in the IMD ecosystem because they mediate communication between implants and cloud services. Since implants do not connect directly to the Internet, attacks instead target the home hub, bedside monitor, smartphone app, or hospital programmer. Reported threats include compromised home hubs, outdated TLS or root certificates, smartphone malware intercepting telemetry, and vulnerable cloud APIs [35, 36, 39]. A compromised home-monitor can send fake configuration packets, eavesdrop on IMD traffic, alter data, or change device behavior. Countermeasures for securing home monitoring in IMDs are shown in Figure 4.

3 METHODOLOGY

3.1 Concept and design of the research methodology

The research methodology for the comparative analysis of security mechanisms used by leading manufacturers of AI-enhanced medical sensors is based on an

integrated risk assessment framework and involves several sequential steps, as illustrated in Figure 5. At its core, the methodology adopts an integrative approach to risk assessment applied for the purposes of the study. This approach consistently integrates the requirements of the medical risk management standard ISO 14971 [43], the risk analysis frameworks NIST SP 800-30 [44] and the security and privacy controls framework NIST SP 800-53 [45], and the analytical hierarchy process AHP, as a multi-criteria decision-making method. The integration ensures full traceability of the assessment process, from the initial threat identification, through the selection and implementation of technical and organizational controls, to the final assessment of the impact on patient safety. Compared to the application of individual frameworks and methods, the proposed integrated methodology provides improved analytical consistency and decision support, thus adding substantial value to the comparative analysis.

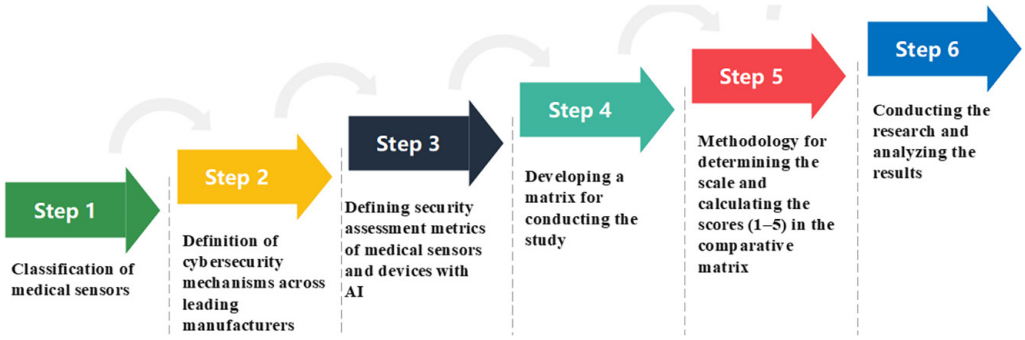

Fig. 5. Basic steps for conducting the study

3.2 Classification of medical sensors

The classification framework presented in Table 1 divides medical AI sensors into primary categories based on their applications, architecture, and security implications, consistent with the study's objectives. This classification allows for a systematic analysis of the specific risks and security needs of each group [1].

Table 1. Classification of medical sensors with integrated AI

	Hospital Multi-Parameter Patches	Outpatient AI-Driven Wearables	Implantable Loop Recorders (ICM/ILR)	Specialty Sensors (CGM, Cardiac Patches)
Typical Devices	GE Portrait Mobile, Philips Biosensor BX100, BioIntelliSense c	iRhythm Zio XT, VitalConnect VitalPatch, Empatica EmbracePlus	Medtronic LINQ II, Abbott Confirm Rx	Dexcom G7 CGM, Abbott Libre 3, Masimo Radius PPG, cardiac ischemia patches
Basic Physiological Signals	HR, RR, SpO_2, temperature, activity, postural changes	ECG (single-lead), PPG, EDA, accelerometry, temperature	ECG	Glucose (interstitial), PPG (SpO_2, HR), multi-channel cardiac signals
Where AI is Implemented	On-device preprocessing + on-gateway analytics + hospital cloud	On-device + mobile app + cloud	Cloud-based AI + clinician interface	Mixed on-device + mobile + cloud
AI Functions	Early warning scores, deterioration prediction, alarm prioritization	Arrhythmia detection, fall detection, seizure analytics, stress/HRV trends	AF detection, arrhythmia burden analytics, long-term cardiac profiling	Trend prediction, hypoglycemia alerts, oxygenation analytics, ischemia/arrhythmia detection

(Continued)

Table 1. Classification of medical sensors with integrated AI *(Continued)*

	Hospital Multi-Parameter Patches	Outpatient AI-Driven Wearables	Implantable Loop Recorders (ICM/ILR)	Specialty Sensors (CGM, Cardiac Patches)
Use Scenarios	Hospital monitoring, continuous observation of patients at risk	Home monito-ring, cardio-logy, neuro-logy, rehabilitation	Long-term cardiac monitoring (years)	Diabetology, intensive care, sports/cardiology medicine
Security Challenges	Hospital Wi-Fi security, firmware integrity, gateway attacks, cloud IAM	BLE security, mobile application, data on smartphone, OTA updates	RF communication security, OTA config, long lifecycle (10+ yrs), home-monitor gateway	BLE security, cloud API threats, mobile app integrity, data poisoning risks

3.3 Definition of cybersecurity mechanisms across leading manufacturers

Security mechanisms, particularly important for implantable and hospital devices where physical access and manipulation are critical [40], can be grouped into six categories:

1. *Hardware and firmware security: secure boot, digitally signed firmware, encrypted storage, and hardware root of trust*;
2. *Secure communication protocols*–AES-128/256, TLS 1.2/1.3, encrypted BLE (LE Secure Connections), and private LTE/5G APNs for hospital hubs;
3. *Cloud security and data management*–GDPR/HIPAA compliance, encryption at rest (AES-256), zero-trust access, audit logging, and device-to-cloud attestation [41];
4. *AI-specific security mechanisms*–model integrity verification, adversarial defenses, drift detection, and secure enclaves for AI execution. Only a few manufacturers (e.g., iRhythm, Medtronic AccuRhythm AI, Empatica) implement such measures, and protections against adversarial attacks and model tampering remain limited [42];
5. *Privacy Protection*–data minimization, (pseudo) anonymization, secure patient ID mapping, and transparent consent management;
6. *Lifecycle Security*–including regular cloud updates and long-term maintenance.

3.4 Defining security assessment metrics

To evaluate and compare the cybersecurity posture of AI-enhanced medical sensor manufacturers, we define a multi-criteria risk-scoring framework based on 10 evaluation criteria. The methodology follows established principles from ISO 14971 [43] (risk management for medical devices), NIST SP 800-30 [44], NIST SP 800-30/53 (risk assessment and security controls) [45], and multi-criteria decision-making (MCDM) approaches, such as the Analytic Hierarchy Process (AHP). We chose 10 criteria.

$$C = \{C_1, C_2, \ldots, C_{10}\} \tag{1}$$

Each manufacturer m receives a discrete score S_m for each criterion C_i ($i \in 1,2,3,4,5$), where higher values indicate better security or safety performance. The ten criteria selected for evaluating AI-enhanced medical sensors reflect the multidimensional nature of safety, performance, and cybersecurity required in modern

clinical environments. Medical sensors with integrated AI operate across multiple layers—signal acquisition, edge processing, wireless telemetry, cloud analytics, and clinical decision support—each introducing distinct risks and reliability considerations. Table 2 presents a traceability matrix that maps each criterion to ISO 14971 activities, applicable NIST SP 800-53 control families, and sample observable indicators for reproducible assessment.

Table 2. Metrics for assessing the security of sensors with integrated AI

Criterion	What is Assessed	Example Observable Indicators	ISO 14971 Linkage	NIST SP 800-53 Families
C1 Crypto & keys	Correct cryptography + key lifecycle	AES-GCM/TLS; key rotation; secure storage; no hardcoded keys	Risk control implementation & verification	SC, IA, CM
C2 Wireless/ session security	Pairing/auth/session protections against radio attacks	Secure pairing; mutual auth; replay protection; unauthorized access	Risk control implementation	AC, IA, SC, AU
C3 AI model security	Robust ML pipeline vs poisoning/adversarial/ model theft	Dataset provenance; adversarial testing; model access control; watermarking/logging	Hazard analysis; risk control evaluation	SI, SA, RA, SR
C4 Cloud & API security	IAM, segmentation, API hardening, monitoring	RBAC; MFA; API rate-limit; audit logs; encryption at rest	Risk control implementation; post-market monitoring	AC, IA, SC, AU, SI
C5 Firmware integrity	Trusted boot + signed updates	Secure boot; signed OTA; anti-rollback; SBOM	Risk control implementation & verification	CM, SI, SA, SC
C6 Physical/ tamper security	Protection vs physical extraction & debug abuse (important for implantable and wearable sensors)	Secure element; JTAG locked; tamper evidence; device attestation	Risk control implementation	PE, SR, MA, SM
C7 Latency/ performance impact	Meeting clinical timing with security enabled -arrhythmia detection, hypoglycemia alerts, deterioration prediction	Worst-case latency; CPU/RAM overhead; graceful degradation	Risk/benefit & residual risk evaluation	SC, SA, SI, SM
C8 Data quality/ integrity	Signal fidelity + integrity vs spoofing/noise	Integrity checks; anomaly detection; calibration; sampling specs	Verification of effectiveness; post-market feedback	SI, SC, AU
C9 Regulatory compliance	Lifecycle evidence of risk & cybersecurity	ISO 14971, IEC 81001-5-1 proc., documentation	Entire ISO 14971 lifecycle	PM, CA, RA, PL,
C10 Clinical safety impact	Safety outcomes & fail-safe behavior, long-term reliability- the determining factor in real-world adoption.	FPR/FNR; alarm fatigue mitigation; fail-safe; reliability metrics	Overall residual risk acceptability	RA, SI, SA

The ten selected criteria cover all layers of an AI-enhanced medical sensor—hardware, firmware, communication, cloud, AI pipeline, and clinical performance—as shown in Figure 6. Together, they provide a balanced framework that encompasses cybersecurity reliability, signal accuracy, regulatory compliance, and real-world clinical safety.

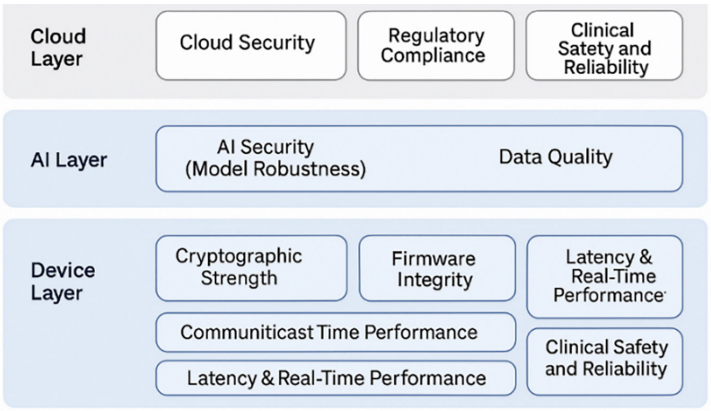

Fig. 6. Criteria by attack layers of sensors with integrated AI

Criteria selection followed a structured standards-to-evidence mapping workflow to ensure transparency and traceability. First, an initial pool of candidate criteria was derived directly from the governing standards: the ISO 14971 risk-management and risk-control lifecycle (including risk control option analysis, implementation, verification of effectiveness, and post-market feedback) and the NIST SP 800-53 control families most applicable to embedded, wireless, and cloud-connected medical/IoMT systems. Second, these candidates were triangulated with recurring themes reported in IoMT cybersecurity surveys and in the AI-for-IoMT security literature to confirm their practical relevance and coverage (e.g., refs. [1], [2], [8], [17], [18]). Third, redundant or overlapping candidates were consolidated and refined through expert judgment (domain review), applying explicit inclusion rules: (a) clear linkage to ISO 14971 and/or NIST SP 800-53, (b) observability/measurability in real systems or public evidence, (c) non-redundancy, and (d) complementary coverage across the main attack surfaces and lifecycle stages. The final set of ten criteria, therefore, provides compact yet comprehensive coverage of hardware and firmware security, wireless communications, cloud/API exposure, the AI/ML pipeline, lifecycle maintenance/updates, and patient/clinical safety, while remaining explicitly grounded in the selected standards through a traceability mapping.

3.5 Threat landscape and attack vectors

Cybersecurity for medical sensors must address risks at multiple levels. They are discussed in detail in section 2.

3.6 Developing a matrix for conducting the research

The matrix has the following columns: Segment, Manufacturer, Device, AI location, AI function, Security technology, Runtime/Battery, Latency, Data quality, and Applicability. Device manufacturers have been added to the rows as: 1. Medtronic,

2. Abbott, 3. Dexcom, 4. GE HealthCare 5. Philips, 6. iRhythm, 7. BioIntelliSense, 8. VitalConnect, 9. Empatica, 10. Masimo.

3.7 Methodology for determining grades (1–5) in the comparison matrix

Method for determining grades. The ratings from 1 to 5 are not random but follow an established academic practice for expert rating used in engineering analysis, cybersecurity, systems engineering, ISO 31000 risk assessments [46], medical device standards IEC 81001-5-1 [37], IEC 62304 [47], and ISO 14971 [43]. The grades are determined using the Expert Judgement Method [48], consisting of:

- *Review of public technical documentation including:* FDA 510(k) documents, security guides, encryption documentation, technical whitepapers, patents, public pages of the compared devices and sensors of popular manufacturers, described in point 3.5 [49, 50, 51, 52, 53, 54, 55, 56, 57, 58], cloud security documents (AWS, Azure, Medtronic CareLink и др.)
- *Academic sources*, peer-reviewed articles, IEEE/ACM publications on medical cybersecurity, BLE/Wi-Fi vulnerability research, and biomedical ML security analysis.
- *Evaluation according to industry standards such as:* the new healthcare cybersecurity standard NIST Cybersecurity Framework, NIST 800-53/800-82 [45], IEC 81001-5-1 [37], ISO 14971:2019 [43], ETSI EN 303 645 [59].
- *Expert interpretation.* The ratings are not provided by the manufacturers, but are analytical assessments based on publicly available information and engineering expertise. These ratings are reasoned, but are not “official” or “certified.” They serve as a scientific comparison, not as a formal certification.

Determining the rating scale from 1 to 5. A maturity scale is used, with the assessment criteria listed in Table 3.

Table 3. Criteria for determining the security ratings of sensors with AI

Assessment	Criterion
Rating 5 – Excellent (full implementation)	The manufacturer has proven, documented, and certified strong cryptography (AES-256, ECC), secure bootloaders, signed firmware, TLS 1.2/1.3, zero-trust cloud, regular security patch cycles, post-market surveillance, and regulated AI models (FDA-cleared). Example: Medtronic LINQ II, Abbott Confirm Rx.
Rating 4 – Very good security, slightly incomplete	The manufacturer has strong implementation, but individual modules are missing, public documentation is limited, or AI security is not fully deployed. Example: GE, Philips, Dexcom, iRhythm.
Rating 3 – Average level	The manufacturer meets basic standards but lacks system AI protections and mechanisms against adversarial attacks; BLE security depends on the phone, and cloud security depends on an external provider. Example: Empatica, Masimo.
Rating 2 – Insufficient	Not used for manufacturers in this analysis because they are medically certified systems. Such devices exhibit significant gaps, lack encryption, have insecure firmware updates, and lack regulatory coverage.
Rating 1 – Minimal, incompatible with medical devices.	Not used for medical devices, this level is typical for consumer IoT devices but not for medical devices.

Calculating the score. For each dimension, a calculation is performed using formula 2:

$$Score = Expert\ Assessment\ of\ (Technocal\ evidence + Regulatory\ Compliance + Security\ Control) \quad (2)$$

For this purpose, the following order is followed:

1. The manufacturer's technical controls are identified, and information is taken from available sources and manufacturers' websites.
2. Documentation is being checked.
3. Compares to industry standards.
4. Expert evaluation is performed on a scale of 1–5.
5. If necessary, the results are normalized.

For example, we give Medtronic a "Crypto Strength" score of 5, after verifying that it has: signed firmware, cryptographically verified telemetry, AES + secure keys in hardware, FDA documentation, and proven security. For Empatica, the score is 3 because it uses a BLE secure connection, but the AI models are cloud-dependent, and there is no formal description of a hardware root of trust. The applied method is completely objective because it uses standards; ratings are based on the same criteria for all; the data are publicly available; no internal or company documents are used; and the analysis is technical and scientific rather than marketing.

4 RESULTS

The results of the sequential implementation of the study steps include: identifying potential attack locations (refer to Table 4), Average WSS by Manufacturer (refer to Table 5), the Security Score heatmap (see Figure 7), the risk-profile ranking (see Figure 8), and the category-level comparison (see Figure 9).

4.1 Mapping the locations of possible attacks

Table 4 summarizes the qualitative mapping of the attack surface across vendors. A consistent trend is that the risk of an AI attack remains at least medium across all vendors, reflecting the evolving nature of adversarial ML threats and the relatively limited public evidence of robust AI-specific defenses. The risk for wireless devices is mostly medium, with one significantly higher case (Empatica) rated high, indicating a higher potential for compromise of the link layer or weaker transport hardening. In contrast, leading vendors focused on implantable devices (e.g., Medtronic, Abbott) show low risk at the physical, firmware, wireless, and cloud layers. This mapping provides practical insight into where greater security assurance is needed: for most vendors, the greatest risks are concentrated in wireless communication, wireless telemetry, and AI channel resilience, while physical-layer threats are relatively better controlled in implantable devices due to tamper-resistant design and mature development processes.

Table 4. Attack surface mapping

Manufacturer	Physical Layer Risk	Firmware Risk	Wireless Risk	Cloud/API Risk	AI Attack Risk
Medtronic	Low	Low	Low	Low	Medium
Abbott	Low	Medium	Low	Low	Medium
Dexcom	Medium	Medium	Medium	Low	Medium
GE	Medium	Medium	Low	Medium	Medium
Philips	Medium	Medium	Low	Medium	Medium
iRhythm	Medium	Medium	Medium	Medium	Medium
BioIntelliSense	Medium	Medium	Medium	Medium	Medium
VitalConnect	Medium	Medium	Medium	Medium	Medium
Empatica	Medium	Medium	High	Medium	Medium
Masimo	Medium	Medium	Medium	Medium	Medium

4.2 Determination of weighted security score for manufacturers

WSS is calculated as a weighted aggregation of C1–C10 scores and is normalized to the range 1–5, allowing direct comparison between manufacturers on a single scale of security/risk profile.

Table 5. Average WSS by manufacturers

Manufacturer	Avg. Score	Strengths	Weaknesses
Medtronic	4.8	High maturity in cryptographic controls and communication security; strong cloud security; very strong firmware integrity and tamper resistance; high data quality protection; strong regulatory compliance and clinical safety.	AI security and latency-related tradeoffs are comparatively less pronounced.
Abbott	4.4	Strong cryptographic, communication, and cloud security; strong data quality protection; high regulatory compliance.	AI security is comparatively weaker; firmware integrity, tamper resistance, and clinical safety remain at a solid but not leading level.
Dexcom	4.0	Secure CGM telemetry, cloud, firmware integrity, tamper resistance, data protection, compliance, and clinical safety.	AI security represents the primary area for further strengthening.
GE	3.8	Balanced and solid performance across most evaluated domains, clinical safety, and strong hospital integration.	AI security and tamper resistance emerge as comparatively weaker dimensions.
Philips	3.8	Balanced and solid performance in most areas assessed, Hospital security.	AI security and tamper resistance emerge.
iRhythm	3.8	Consistent and robust security and clinical safety profile. End-to-end ECG analytics, FDA-cleared AI pipelines	Firmware integrity and tamper resistance

(Continued)

Table 5. Average WSS by manufacturers *(Continued)*

Manufacturer	Avg. Score	Strengths	Weaknesses
BioIntelliSense	3.6	Solid performance in cryptography, cloud security, latency tradeoff, data quality protection, compliance, and clinical safety.	Communication and AI security, firmware integrity, and tamper resistance.
VitalConnect	3.6	Solid cryptographic, communication, cloud security, data protection, and clinical safety.	AI security, firmware integrity, tamper resistance, and latency tradeoff.
Empatica	3.3	Solid cloud security, data quality protection, and regulatory compliance.	Cryptography, communication, AI security, firmware integrity, tamper resistance, latency tradeoff, and clinical safety.
Masimo	3.3	Solid latency tradeoff, data quality protection, and regulatory compliance. PPG robustness	Cryptography, communication, AI, cloud security, firmware integrity, tamper resistance, and clinical safety.

According to the results in Table 5, three distinct groups are formed. The leading group, which includes manufacturers such as Medtronic (4.8), Abbott (4.4), and Dexcom (4.0), has the highest security. The middle group (GE, Philips, iRhythm – 3.8 each) shows balanced but not leading security. For these manufacturers, AI security and/or resistance to unauthorized access are relatively weaker dimensions, and for iRhythm, gaps in firmware integrity and resistance to unauthorized change are also observed. The third group (BioIntelliSense and VitalConnect – 3.6 each; Empatica and Masimo – 3.3 each) shows more limited maturity or inconsistency of protections: for BioIntelliSense the weaknesses are in communication security, AI security, firmware integrity and tampering, for VitalConnect it is the trade-off between AI, firmware, tampering and latency for Empatica – weaknesses are present in almost all key areas (including cryptography and communications), and for Masimo – despite the strengths in the trade-off with latency/data/compliance, weaknesses are observed in cryptography/communications/AI/cloud/firmware/tampering and clinical safety.

A key result is that the most common "weak area" among vendors is AI security (C3), followed by hardware tamper resistance (C6) and firmware integrity (C5). This is important because these areas directly affect the reliability of the algorithmic solution, the resistance to manipulation, and the risk of device compromise. The connection to Table 4 is direct: the attack surface mapping (NIST SP 800-30) shows the attack vectors by layer, and Table 5 shows the extent to which individual vendors address these vectors through robust controls at critical layers (device/firmware, wireless, cloud/API, and AI pipeline).

The Security Score Heatmap is shown in Figure 7.

Figure 7 visualizes the criteria-level scores as a heat map, revealing where gaps are systematic rather than vendor-specific. Among the lowest-rated criteria is AI Security, suggesting that model integrity, adversarial system resilience, and ML pipeline hardening are not yet at the same level of maturity as traditional cryptographic and cloud controls. The heat map also shows that strong cryptography and cloud governance alone do not guarantee high overall security if firmware integrity, secure update mechanisms, and AI-specific protections remain moderate.

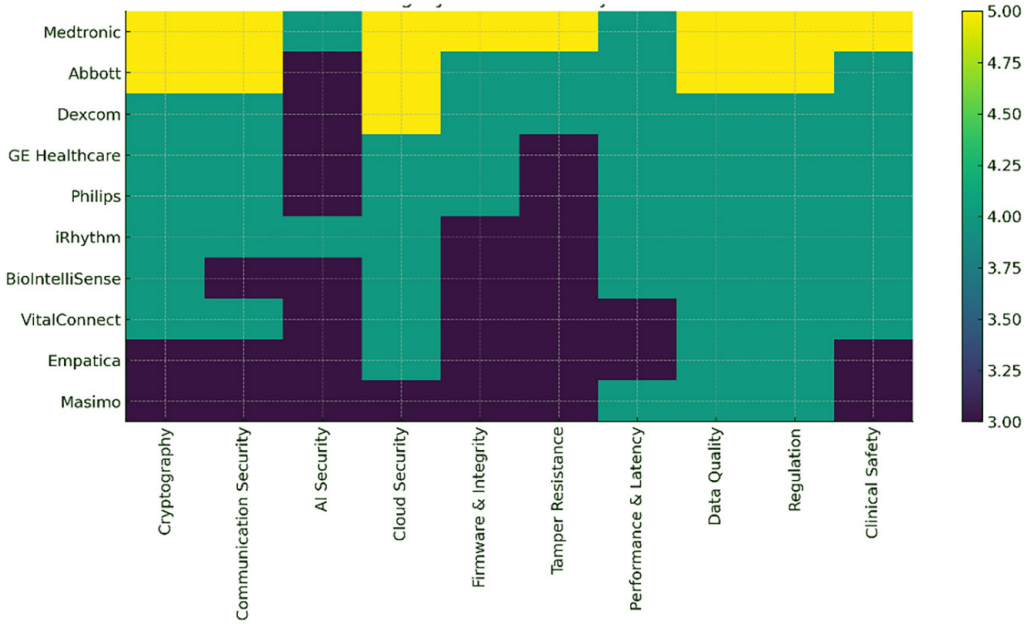

Fig. 7. Weighted security score heatmap by manufacturer

4.3 Risk profile ranking

Determining weights. The risk profile is calculated as a weight × score for each criterion. The weights determine how strongly a given criterion contributes to overall risk (patient safety impact and the likelihood of exploitation). The weight values are derived from international standards for medical-device risk management and cybersecurity, complemented by an AHP-style pairwise comparison procedure. The resulting weights are summarized in Table 6 and visualized in Figure 8.

$$\omega_i \geq 0, \sum_{i=1}^{10} \omega_i = 1 \tag{3}$$

The weights reflect the relative contribution of each criterion to the overall risk and are derived using a hybrid approach:

- *Impact-probability* assessment according to ISO 14971 and NIST SP 800-30, shows how seriously a violation of this criterion affects patient safety or data protection, and the probability—how realistic it is that this criterion will be attacked or fail in real-world application.
- *Expert pairwise comparison (AHP-style).* Subject-matter experts (cybersecurity, clinical engineering, regulatory affairs) perform pairwise comparisons between criteria (e.g., "Cryptographic Strength vs. Latency") to determine which is more important and by how much. These comparisons form a pairwise comparison matrix A = (a_{ij}), where:

$$a_{ij} = \begin{cases} 1 & \text{if } C_i \text{ and } C_j \text{ are equally important} \quad 0 \\ >1 & \text{if } C_i \text{ is more imporment than } C_j \quad 0 \\ 0<1 & \text{if } C_i \text{ is less imporment than } C_j \quad 0 \end{cases} \tag{4}$$

The weights reflect the priorities outlined in the FDA cybersecurity guidelines (e.g., cryptographic integrity, secure update mechanisms, and cloud/API security) and in IEC 81001-5-1. Criteria related to encryption, communications, and cloud security receive slightly higher final weights. Example: Cryptographic strength, weight 0.15, has a high weight because cryptography protects the entire data channel. There is a trade-off between latency (0.05) and low weight, because it affects response speed but not safety [48].

Table 6. Determining the weights for the risk profile

Criterion	Weight	Criterion	Weight
ω_1 (Strength)	0.15	ω_6 (Tamper Resistance)	0.10
ω_2 (Com. Security)	0.15	ω_7 (Latency Tradeoff)	0.05
ω_3 (AI Security)	0.10	ω_8 (Data Quality)	0.05
ω_4 (Cloud Security)	0.15	ω_9 (Reg. Compliance)	0.10
ω_5 (Firmware Integ.)	0.10	ω_{10} (Clinical Safety)	0.05

The higher the *Risk Profile Score*, the safer and less risky the manufacturer. The ranking looks like this (according to the calculated values): Medtronic—highest overall score; Abbott, Dexcom, Philips, GE Healthcare, Masimo—highest risk profile (lowest protection).

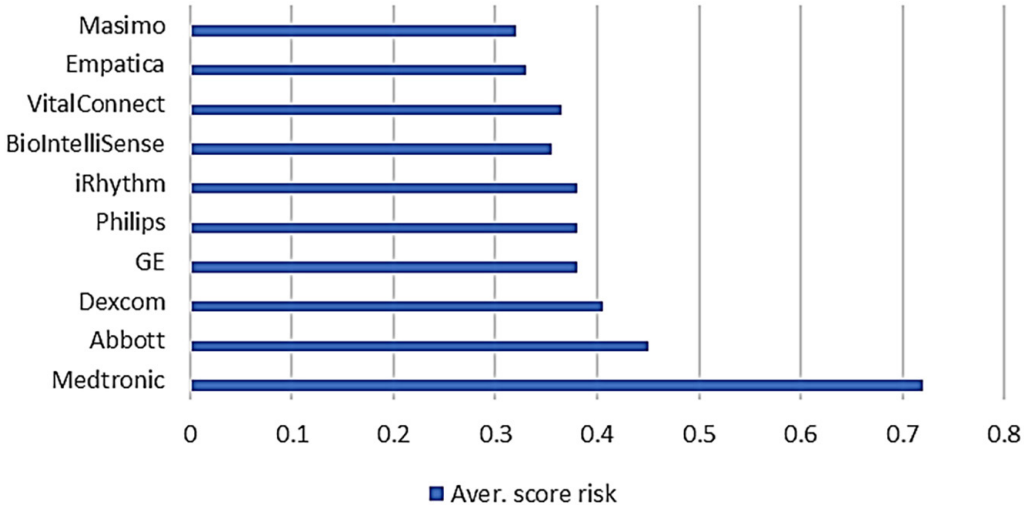

Fig. 8. Risk profile ranking (weighted score)

4.4 Comparison per category

Figure 9 compares average security scores across device categories. Implantable devices exhibit the highest overall security maturity, reflecting stringent regulatory oversight, hardened physical/firmware integrity, and long-term lifecycle management. CGM systems and ambulatory wearables show strong performance in data-quality protection and cloud connectivity, but remain constrained by wireless exposure and AI-security maturity. Hospital patches and multi-parameter platforms

benefit from controlled clinical environments, yet their broader connectivity and integration surfaces can increase risks related to cloud/APIs and gateways.

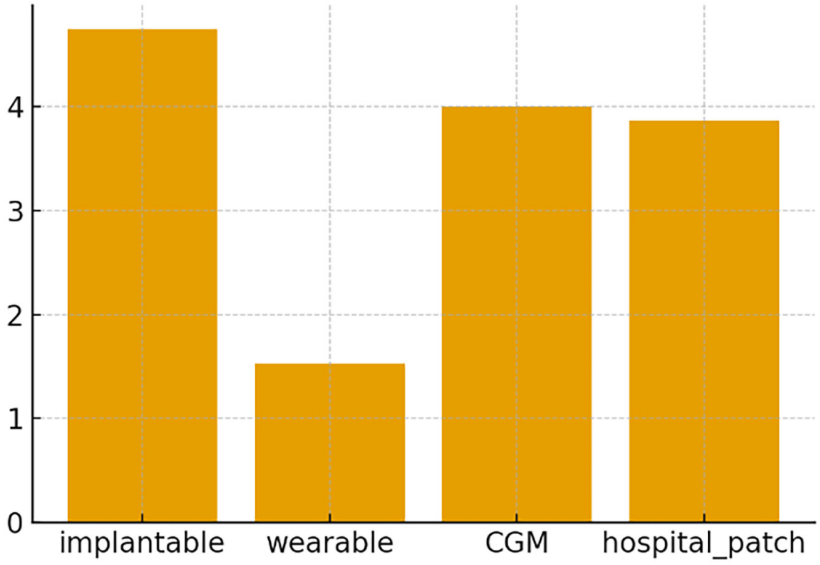

Fig. 9. Average security score per device category

5 DISCUSSIONS

The results of this study support prior literature on IoMT, highlighting that connected medical sensors are exposed to increased risk due to heterogeneous protocols, limited device resources, and insufficient authentication and security mechanisms [1–3]. The layer-by-layer identification of threats and vulnerabilities, followed by attack surface mapping (refer to Table 4), directly supports previous system-level perspectives that advocate for continuous monitoring, real-time threat detection, and architectural risk visibility in IoMT environments [11, 12]. In particular, our mapping highlights that risk is rarely located in a single component; rather, it accumulates across the device/firmware layer, wireless connectivity, and cloud/API dependencies. A key finding from the vendor-level comparison (refer to Table 5, WSS on a scale of 1–5) is that security maturity varies significantly across vendors, confirming previous observations that cybersecurity capabilities and risk management practices are not uniform across leading vendors and that a systematic comparative view is needed ([8], [10]). The WSS results further clarify which areas most often limit the overall position: AI security repeatedly emerges as the dominant weakness across multiple vendors, followed by firmware integrity and tamper resistance. This is consistent with studies noting that many existing risk assessment approaches focus on device/network behavior or regulatory checklists, while not paying sufficient attention to AI-specific threats such as data poisoning, adversary manipulation, and training data compromise [13], [14]. The conclusion is that "secure communication" per se (e.g., AES/TLS/secure BLE) is necessary but not sufficient; when AI components shape clinical decisions, the AI pipeline becomes a first-class attack surface that requires explicit protection and validation.

IoMT security research [15] identifies two closely related gaps: first, the need for comprehensive operational risk assessment and management frameworks that span

all layers of IoMT architectures, and second, the persistent difficulty in creating meaningful quantitative security/risk assessments, as many proposals remain qualitative, threat-specific, or IDS-centric, rather than comprehensive and measurable. Building on the above findings and observations, our study provides a standards-based and reproducible workflow that integrates ISO 14971 with NIST SP 800-30/800-53 and a multi-criteria decision analysis approach to transform multi-layered evidence of the attack surface into quantitative prioritization and comparable benchmarking (average WSS values at the vendor and device category levels).

Analyzing the results of the research, we can conclude that there that there is a clear trend for the "AI Security" criterion to be among the lowest rated for most manufacturers (often 3/5), which points to a systemic need for more mature measures for AI model resilience, drift risk management, and protection of the ML/AI chain (pipeline). In parallel, "Firmware Integrity" and "Tamper Resistance" stand out as recurring areas for improvement for some suppliers, especially those with more even but not maximum profiles. In contrast, "Regulatory Compliance" and "Data Quality Protection" are rated relatively high and more consistently (usually 4–5/5), suggesting better institutionalized practices in domains related to regulatory frameworks and the protection of clinically relevant data.

Among the companies considered, Medtronic demonstrates the highest maturity across almost all dimensions, with only latency-oriented trade-offs and AI security remaining at "very good," not at maximum levels. Abbott shows a strong profile in cryptography, communication, and cloud security and regulatory compliance, but AI security is relatively weaker. Dexcom stands out with a high score for cloud security, with generally stable results in the other criteria, while GE and Philips demonstrate a balanced "solid" picture with lower scores in AI security and physical tamper resistance. iRhythm's profile is even and stable, but lower scores stand out in firmware integrity and tamper resistance, while BioIntelliSense and VitalConnect show a moderate level of maturity with a concentration of weaknesses in communication security/AI and firmware-physical protection. Empatica and Masimo have lower overall profiles across more areas, primarily because they focus on clinical functionality rather than AI/cybersecurity. They maintain relatively strong positions in data quality protection and regulatory compliance, but show pronounced deficiencies in core technical controls (crypto, communications, firmware, and tamper protection).

Finally, regarding segment differences: Implantables have the highest security requirements; CGM systems are strong in data quality; hospital patches rely on infrastructure; and wearables are most vulnerable to cloud and mobile threats.

6 CONCLUSION

Based on the research conducted, we confirm the importance of the cybersecurity of AI-enhanced medical sensors. We prove this confirmation through the development:

First, an integrated methodology for assessing security maturity that combines the principles of ISO 14971, NIST SP 800-30/53, and the AHP expert approach. Definition of ten weighted criteria, providing an objective framework for analyzing cyber risks in different classes of medical devices - multi-parameter hospital patches, ambulatory wearable devices, implantable systems, and CGM monitors.

Second, a comparative analysis of ten leading manufacturers was conducted, generating two key indices: a combined weighted security score (WSS) and a RPS.

These indices enable an objective ranking of the level of protection and exposure to vulnerabilities, including those arising from increasingly integrated AI models within these devices.

Third, identifying critical security vulnerabilities, including insufficient protection of AI modules against manipulation, reduced resilience of wireless communication in ambulatory wearable devices, and differences in cryptographic practices between manufacturers.

Fourth, the results are valuable for designers of medical sensors and for clinicians who use the devices in real practice. The proposed methodology can also be used in the educational environment – for preparing students in biomedical engineering, medical informatics, and health technologies, as well as a practical framework for training in risk assessment and cybersecurity in medical systems.

Finally, to address these shortcomings, it is advisable to introduce unified standards and policies for AI and security across the entire life cycle of medical sensor devices.

7 REFERENCES

[1] A. Naghib, F. Gharehchopogh, and A. Zamanifar, "A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: Current status, challenges, and opportunities," *Artif. Intell. Rev.*, vol. 58, p. 114, 2025. https://doi.org/10.1007/s10462-024-11101-w

[2] S. Messinis, N. Temenos, N. E. Protonotarios, I. Rallis, D. Kalogeras, and N. Doulamis, "Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review," *Comput. Biol. Med.*, vol. 170, p. 108036, 2024. https://doi.org/10.1016/j.compbiomed.2024.108036

[3] F. Tsvetanov, "Hardware challenges in AI sensors and innovative approaches to overcome them," *Eng. Proc.*, vol. 104, no. 1, p. 19, 2025. https://doi.org/10.3390/engproc2025104019

[4] F. Tsvetanov, "Integrating AI technologies into remote monitoring patient systems," *Eng. Proc.*, vol. 70, no. 1, p. 54, 2024. https://doi.org/10.3390/engproc2024070054

[5] I. T. Al-Haboosi, B. M. Elbagoury, S. El-Regaily, and E.-S. M. El-Horbaty, "A hybrid-transformer-based cyber-attack detection in IoT networks," *Int. J. Interact. Mobile Technol.*, vol. 18, no. 14, pp. 90–102, 2024. https://doi.org/10.3991/ijim.v18i14.50343

[6] F. A. Tsvetanov and M. N. Pandurski, "Security of the sensory data in the cloud," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 1032, no. 1, p. 012005, 2021. https://doi.org/10.1088/1757-899X/1032/1/012005

[7] V. Rattanawiboomsom, M. S. Korejo, J. Ali, and U. Thatsaringkharnsakun, "Blockchain-enabled Internet of Things (IoT) applications in healthcare: A systematic review of current trends and future opportunities," *Int. J. Online Biomed. Eng.*, vol. 19, no. 10, pp. 99–117, 2023. https://doi.org/10.3991/ijoe.v19i10.41399

[8] M. Hernandez-Jaimes, A. Martínez-Cruz, K. Ramírez-Gutiérrez, and C. Uribe, "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures," *Internet of Things*, vol. 23, p. 100887, 2023. https://doi.org/10.1016/j.iot.2023.100887

[9] E. Biasin, E. Kamenjašević, and K. R. Ludvigsen, "Cybersecurity of AI medical devices: Risks, legislation, and challenges," in *Research Handbook on Health, AI and the Law*, 2024, pp. 57–74. https://doi.org/10.4337/9781802205657.ch04

[10] I. Brass and A. Mkwashi, "Risk assessment and classification of medical device software for the internet of medical things: Challenges arising from connected, intelligent medical devices," in *Proc. 12th Int. Conf. on the Internet of Things*, 2022, pp. 171–178. https://doi.org/10.1145/3567445.3571104

[11] R. M. Alharbi and M. A. Khan, "Analyzing cyber attack detection in IoT healthcare environments using artificial intelligence," *Int. J. Advanced Computer Science & Applications*, vol. 16, no. 8, 2025. https://doi.org/10.14569/IJACSA.2025.0160841

[12] K. Kioskli, E. Grigoriou, S. Islam, A. M. Yiorkas, L. Christofi, and H. Mouratidis, "A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain," *Int. J. Information Security*, vol. 24, no. 2, pp. 1–28, 2025. https://doi.org/10.1007/s10207-025-01009-z

[13] B. S. Kelly, C. Quinn, N. Belton, A. Lawlor, R. P. Killeen, and J. Burrell, "Cybersecurity considerations for radiology departments involved with artificial intelligence," *European Radiology*, vol. 33, no. 12, pp. 8833–8841, 2023. https://doi.org/10.1007/s00330-023-09860-1

[14] A. Arafa, H. A. Sheerah, and S. Alsalamah, "Emerging digital technologies in healthcare with a spotlight on cybersecurity: A narrative review," *Information*, vol. 14, no. 12, p. 640, 2023. https://doi.org/10.3390/info14120640

[15] K. Svandova and Z. Smutny, "Internet of medical things security frameworks for risk assessment and management: A scoping review," *Journal of Multidisciplinary Healthcare*, vol. 17, pp. 2281–2301, 2024. https://doi.org/10.2147/JMDH.S459987

[16] V. Gomase, A. Ghatule, R. Sharma, and S. Sardana, "Cybersecurity and compliance in clinical trials: The role of artificial intelligence in secure healthcare management," *Rev. Recent Clin. Trials*, vol. 20, no. 4, pp. 332–351, 2025. https://doi.org/10.2174/0115748871366467250413070850

[17] M. K. Hasan *et al.*, "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things," *IET Commun.*, vol. 16, no. 5, pp. 421–432, 2021. https://doi.org/10.1049/cmu2.12301

[18] A. A. Pise *et al.*, "Enabling artificial intelligence of things (AIoT) healthcare architectures and listing security issues," *Comput. Intell. Neurosci.*, vol. 2022, no. 1, p. 8421434, 2022. https://doi.org/10.1155/2022/8421434

[19] A. Si-Ahmed, M. Al-Garadi, and B. Narhimene, "Survey of machine learning–based intrusion detection methods for Internet of Medical Things," *Appl. Soft Comput.*, vol. 140, p. 110227, 2023. https://doi.org/10.1016/j.asoc.2023.110227

[20] R. Agrawal, P. S. Rathore, G. G. Deverajan, and R. R. Divivedi, *Artificial Intelligence and Cybersecurity in Healthcare*. Hoboken, NJ, USA: John Wiley & Sons, 2025. https://doi.org/10.1002/9781394229826

[21] M. Terzidis *et al.*, "Challenges in Medical Device Communication," in *Proc. CYBER* 2023, pp. 25–29.

[22] Gattacker, "A Node.js Package for BLE Man-in-the-Middle & More," 2025. https://github.com/gattacker

[23] BlueGoat Cyber, "SoC vulnerabilities in medical devices: What manufacturers need to know," 2025. https://bluegoatcyber.com/blog/exploring-system-on-a-chip-soc-vulnerabilities

[24] The Knowledge Academy, "What is deadlock in OS?" 2025. https://www.theknowledgeacademy.com/blog/deadlock-in-os

[25] R. Katsuya and X. Liu, "Policy and management implications of firmware vulnerabilities in medical IoT devices: A multi-case analysis," *J. Sci. Technol. Policy Manag.*, 2025. https://doi.org/10.1108/JSTPM-09-2024-0346

[26] S. Taheri and N. Asadizanjani, "An overview of medical electronic hardware security and emerging solutions," *Electronics*, vol. 11, no. 4, p. 610, 2022. https://doi.org/10.3390/electronics11040610

[27] J. Davis, "Healthcare FHIR'd up: Addressing security flaws in the API ecosystem," 2025. https://www.scworld.com/feature/healthcare-fhird-up-addressing-security-flaws-in-the-api-app-ecosystem

[28] S. Alder, "Warning issued about access:7 Vulnerabilities affecting IoT and medical devices," *HIPAA Journal*, Mar. 9, 2022. https://www.hipaajournal.com/warning-issued-about-access7-vulnerabilities-affecting-iot-and-medical-devices

[29] S. G. Finlayson, J. D. Bowers, J. Ito, J. L. Zittrain, A. L. Beam, and I. S. Kohane, "Adversarial attacks on medical machine learning," *Science*, vol. 363, no. 6433, pp. 1287–1289, 2019. https://doi.org/10.1126/science.aaw4399

[30] T. Ino, K. Yoshida, H. Matsutani, and T. Fujino, "Data poisoning attack against neural network-based on-device learning anomaly detector by physical attacks on sensors," *Sensors*, vol. 24, no. 19, p. 6416, 2024. https://doi.org/10.3390/s24196416

[31] Health Sector Council, "HIC-AIM," 2023. https://healthsectorcouncil.org/health-industry-cybersecurity-artificial-intelligence-machine-learning/

[32] A. Kore *et al.*, "Empirical data drift detection experiments on real-world medical imaging data," *Nat. Commun.*, vol. 15, p. 1887, 2024. https://doi.org/10.1038/s41467-024-46142-w

[33] A. Mitra and D. Roy Chowdhury, "A secure data transmission protocol for cardiac implants to mitigate intrusive cyber attacks," in *Cybersecurity*, L. Praça, S. Bernardi, P. R. Inácio, Eds., vol. 2500, Cham, Switzerland: Springer, 2025, pp. 307–323. https://doi.org/10.1007/978-3-031-94855-8_20

[34] D. Ismail, "Securing implantable medical devices against remote attacks by anomaly detection: Enhancing IoT security within healthcare," Master's thesis, KTH Royal Institute of Technology, 2024. https://www.diva-portal.org/smash/get/diva2:1935815/FULLTEXT01.pdf

[35] M. Ouaissa and M. Ouaissa, "Analyzing and mitigating attacks in IoT smart home using a threat modeling approach-based STRIDE," *Int. J. Interact. Mob. Technol.*, vol. 19, no. 2, pp. 126–142, 2025. https://doi.org/10.3991/ijim.v19i02.52377

[36] U.S. Food and Drug Administration, *Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions: Guidance for Industry and Food and Drug Administration Staff*. Silver Spring, MD, USA: U.S. Food and Drug Administration, Feb. 2026. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-management-system-considerations-and-content-premarket

[37] IEC, "IEC 81001-5-1:2021 – Health software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product life cycle," 2021.

[38] D. Bhavani and V. Raju, "A Panoptic of Vulnerabilities in Implantable Medical Devices," *SSRN Electron. J.*, 2023. https://doi.org/10.2139/ssrn.4322237

[39] M. Ngamboé *et al.*, "Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED)," *Int. J. Inf. Secur.*, vol. 20, pp. 621–645, 2019. https://doi.org/10.1007/s10207-020-00522-7

[40] F. Oikonomou *et al.*, "Blockchain-based security mechanisms for IoMT edge networks," *Sensors*, vol. 22, no. 7, p. 2449, 2022. https://doi.org/10.3390/s22072449

[41] M. Wazid, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and M. Guizani, "AISCM-FH: AI-enabled secure communication mechanism in fog computing-based healthcare," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 319–334, 2023. https://doi.org/10.1109/TIFS.2022.3220959

[42] H. Javed, S. El-Sappagh, and T. Abuhmed, "Robustness in deep learning models for medical diagnostics: Security and adversarial challenges," *Artif. Intell. Rev.*, vol. 58, p. 12, 2024. https://doi.org/10.1007/s10462-024-11005-9

[43] ISO, "ISO 14971:2019 – Medical devices – Application of risk management to medical devices," 2019.

[44] NIST SP 800-30 Rev. 1, "Guide for Conducting Risk Assessments," 2012. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[45] NIST, "Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5)," *Gaithersburg*, 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[46] ISO, "ISO 31000:2018 risk management — guidelines," 2018. https://www.iso.org/standard/65694.html

[47] IEC, "IEC 62304:2006+A1:2015. Medical device software — Software life cycle processes," 2015. https://doi.org/10.1049/ic:20060141

[48] N. Moghadasi *et al.*, "Risk analysis of artificial intelligence in medicine with a multilayer concept of system order," *Systems*, vol. 12, no. 2, p. 47, 2024. https://doi.org/10.3390/systems12020047

[49] Medtronic, "LINQ II™ Insertable Cardiac Monitor," https://www.medtronic.com/en-us/healthcare-professionals/products/cardiac-rhythm/cardiac-monitoring/insertable-cardiac-monitors/linq-ii-icm.html

[50] Abbott, "Confirm Rx™ Insertable Cardiac Monitor with SharpSense™ Technology," Abbott Cardiovascular. https://www.cardiovascular.abbott/int/en/hcp/products/cardiac-rhythm-management/insertable-cardiac-monitors/confirm-rx.html

[51] Dexcom, "Dexcom G7 Continuous Glucose Monitoring System," Dexcom. https://www.dexcom.com/en-us/g7-cgm-system

[52] GE HealthCare, "Portrait™ Mobile: Wireless and Wearable Monitoring Solution," GE HealthCare. https://www.gehealthcare.com/-/jssmedia/gehc/us/files/products/patient-monitoring/brochure-portrait-mobile-jb16385xx_v4.pdf

[53] Philips, "Philips Biosensor BX100: A wearable device for remote respiratory rate monitoring," Philips Healthcare. https://www.philips.com/c-dam/b2bhc/master/Specialties/general-care-general-ward/bx-100-rr-whitepaper.pdf

[54] iRhythm Technologies, "Zio XT Long-Term Continuous Monitor," iRhythm Technologies. https://www.irhythmtech.com/gb/en/healthcare-professionals/monitoring

[55] BioIntelliSense, "BioButton Multi-Parameter Continuous Vital Sign Monitor," https://www.biointellisense.com/biobutton

[56] VitalConnect, "VitalPatch® RTM," VitalConnect. https://vitalconnect.com/cardiac-monitoring/

[57] Empatica, "EmbracePlus," 2026. https://www.empatica.com/embraceplus

[58] Masimo, "Radius PPG® Tetherless Pulse Oximetry," Masimo. https://www.masimo.com/products/wearables/radius-ppg/

[59] ETSI, "ETSI EN 303 645 V3.1.3 — Cyber Security for Consumer Internet of Things: Baseline Requirements," 2024. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

8 AUTHOR

Filip Tsvetanov has a PhD and is a University lecturer, researcher, and expert in ICT and security of computer and sensor networks, in the Department of Communication and Computer Engineering and Technologies in the Faculty of Engineering, with research in the field encompassing telecommunications, computer and sensor networks, and the security of transmitted data and networks (E-mail: ftsvetanov@swu.bg).