Internet of Things 40 (2026) 102085

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Research article

Security and risk assessment of IoMT communication protocols: A data-driven analysis of real-world vulnerabilities

Charalampos Sergiou [a,*], Costas Iordanou [a], Konstantinos Katzis [a], Gregory Epiphaniou [b,c], Nabil Moukafih [b], Carsten Maple [b,d], Nikolaos Matragkas [e], Marcos Didonet del Fabro [e]

[a] Department of Computer Science and Engineering, European University Cyprus, Nicosia, Cyprus
[b] Secure Cyber Systems Research Group, University of Warwick, United Kingdom
[c] Information Computer Science Department, King Fahd University of Petroleum Minerals (KFUPM), Saudi Arabia
[d] Alan Turing Institute, United Kingdom
[e] Université Paris-Saclay, CEA-List, France

ARTICLE INFO

Keywords:
Internet of medical things (IoMT)
Communication protocol security
Risk assessment
Cybersecurity in healthcare
Mitigation strategies

ABSTRACT

The Internet of Medical Things (IoMT) comprises interconnected medical devices and systems that monitor patients, exchange physiological data, and support clinical decision making through diverse wireless protocols. Although this connectivity improves healthcare efficiency and precision, the coexistence of resource constrained and safety critical devices creates cybersecurity and privacy challenges. This study presents a reproducible comparative vulnerability analysis of Bluetooth Low Energy, Zigbee, Wi-Fi, LoRaWAN, and proprietary radio frequency telemetry. The analysis combines qualitative threat characterization with quantitative assessment of a protocol oriented sample constructed from the National Vulnerability Database JSON 2.0 year feeds labelled 2020 to 2025. Mean CVSS v3.x Exploitability and Impact subscores were normalized against their maxima and combined into a descriptive baseline composite index. Deployment exposure was considered separately through specified noncalibrated scenario multipliers. Analysis of 4378 retained CVEs produced baseline composite indices ranging from $R = 0.378$ to $R = 0.562$. Differences in Exploitability distributions did not meet the significance threshold, with $p = 0.0561$ and a negligible effect size. In contrast, Impact distributions differed statistically, with $p < 0.001$ and a modest effect size, while Wi-Fi showed the clearest elevated Impact profile. The scenario analysis proportionally rescaled the indices without changing the protocol ordering. As the scenario parameters were not calibrated using operational healthcare data, the resulting values should not be interpreted as measured hospital or home care risk. The findings can inform comparative vulnerability prioritization, mitigation planning, and interpretation of deployment conditions in IoMT systems.

* Corresponding author.
E-mail addresses: c.sergiou@research.euc.ac.cy (C. Sergiou), C.Iordanou@euc.ac.cy (C. Iordanou), K.Katzis@euc.ac.cy (K. Katzis), Gregory.Epiphaniou@warwick.ac.uk (G. Epiphaniou), Nabil.Moukafih@warwick.ac.uk (N. Moukafih), CM@warwick.ac.uk (C. Maple), Nikolaos.Matragkas@cea.fr (N. Matragkas), Marcos.Didonetdelfabro@cea.fr (M. Didonet del Fabro).

https://doi.org/10.1016/j.iot.2026.102085
Received 12 November 2025; Received in revised form 26 August 2026; Accepted 27 August 2026
Available online 31 August 2026

1. Introduction

The Internet of Medical Things (IoMT) represents a rapidly evolving ecosystem of healthcare technologies that interconnect medical devices, embedded sensors, wireless networks, and cloud-based services to enable real-time data exchange and continuous patient monitoring [1]. This convergence of biomedical engineering and wireless communication has reshaped preventive healthcare, telemedicine, and data-driven clinical decision-making. Devices such as wearable trackers, implantable sensors, infusion pumps, and diagnostic instruments are increasingly integrated into smart environments or directly attached to the human body, forming a cornerstone of modern digital healthcare [2]. Unlike conventional IT systems, IoMT environments operate under stringent safety and regulatory constraints. Devices must sustain real-time responsiveness and high availability while handling sensitive physiological data, often without direct human supervision. Many operate in uncontrolled settings, such as patient homes or public facilities, where connectivity is unreliable and network protection is not sufficient. Furthermore, physical limitations in processing power, memory, and energy capacity restrict the use of computationally intensive cryptographic mechanisms, rendering security configuration a critical design trade-off [3].

While IoMT connectivity enhances clinical functionality, the underlying protocol heterogeneity introduces a complex cybersecurity landscape. Communication standards such as Bluetooth Low Energy (BLE), Zigbee, Wi-Fi, and LoRaWAN, although efficient and interoperable, are primarily designed for consumer or industrial environments, rather than safety-critical healthcare contexts [4]. As a result, adversaries exploit protocol-level weaknesses to intercept telemetry, disrupt clinical workflows, or compromise firmware integrity [5]. Exposure to untrusted networks further amplifies these risks. Home-based or mobile health devices often connect through open access points and remain physically accessible to attackers. Weak encryption, insufficient authentication, or insecure update mechanisms create entry points for unauthorized access. Once compromised, a device can serve as a pivot into hospital infrastructures or inject falsified sensor readings, potentially leading to diagnostic errors or unsafe therapeutic actions [6]. The fragmented IoMT ecosystem, marked by vendor heterogeneity, proprietary firmware, and irregular patch cycles, complicates coordinated defense. Moreover, regulatory obligations may delay firmware updates or restrict design modifications, producing operational inertia in incident response. These challenges underscore the need for a risk-oriented and context-aware approach to IoMT communication security, one that evaluates not only the technical robustness of each protocol but also its operational exposure and clinical criticality [7].

To address these needs, this study presents a structured and comparative security assessment of five major IoMT communication protocols: Bluetooth Low Energy (BLE), Zigbee, Wi-Fi, LoRaWAN, and proprietary RF telemetry. The analysis combines qualitative threat modeling with quantitative evaluation based on vulnerability data extracted from the National Vulnerability Database[1] (NVD, 2020–2025). By mapping protocol-related vulnerabilities and deriving comparative Likelihood and Impact indicators, the study provides a transparent and reproducible framework for risk-informed protocol evaluation in healthcare networks. This approach complements existing protocol surveys and IoT/IoMT security reviews by adding a comparative, evidence-based perspective on communication-layer risk. Rather than proposing a new communication protocol, security mechanism, or standalone theoretical risk model, this study contributes a reproducible empirical cross-protocol security analysis based on a protocol-oriented sample derived from the NVD JSON 2.0 year feeds labelled 2020 through 2025. The analysis goes beyond protocol-level mean comparison by examining the distributions of CVSS Exploitability and Impact subscores, quantifying uncertainty in the resulting protocol-level estimates, and statistically evaluating whether the observed differences across communication technologies are supported by the underlying vulnerability data. The contribution therefore lies in the integration of large-scale vulnerability evidence, statistical cross-protocol comparison, uncertainty assessment, and deployment-aware interpretation for IoMT communication environments.

The main contributions of this study are summarized as follows:

- A reproducible cross-protocol analysis of a protocol-oriented sample derived from the NVD JSON 2.0 year feeds labelled 2020 through 2025 is performed for five communication technologies relevant to IoMT, resulting in 4378 retained CVE records with valid CVSS v3.x Exploitability and Impact subscores.
- Protocol-level vulnerability evidence is evaluated beyond mean-score comparison through descriptive statistics, bootstrap confidence intervals, non-parametric Kruskal–Wallis testing [8], ordinal eta-squared effect-size analysis [9,10], and, where warranted by a statistically significant omnibus result, post-hoc Dunn comparisons [11] with Holm correction [12]. The complete mathematical formulation of these procedures is provided in Appendix A.
- A common data-derived baseline is established through normalized Exploitability–Impact indices, while deployment-dependent assumptions are separated from the empirical baseline and examined independently through scenario-specific analysis.
- The quantitative findings are linked to protocol-specific security characteristics and mitigation requirements across hospital, home-care, and constrained or implantable-device environments, providing practical support for vulnerability prioritization, protocol configuration, and communication-layer risk management.

The rest of the paper is organized as follows. Section 2 reviews related work. Section 3 describes IoMT communication protocols. Section 4 analyzes protocol-specific threats and vulnerabilities. Section 5 introduces and empirically evaluates the risk-assessment methodology, and Section 6 presents deployment-aware mitigation strategies. Section 7 discusses the cross-protocol findings, their practical implications, and the limitations of the analysis. Section 8 concludes the paper and outlines directions for future research.

[1] https://nvd.nist.gov/

2. Related work

The rapid growth of IoMT has motivated extensive research on communication architectures, security challenges, and mitigation frameworks. Surveys by Verma et al. [4] and Shaikh et al. [13] provide comprehensive overviews of IoMT system components and network topologies, emphasizing how heterogeneous communication standards complicate interoperability and introduce inconsistent trust assumptions across healthcare platforms. These studies collectively underline the need for adaptable security solutions that consider the operational constraints and communication profiles of individual protocols.

Protocol-specific vulnerabilities have been examined in several works. In [14], the authors identified major weaknesses in Bluetooth Low Energy (BLE), including unauthenticated pairing and unencrypted communication modes prevalent in commercial devices. Bellardo and Savage [15] analyzed Wi-Fi's susceptibility to denial-of-service (DoS) and signal-jamming attacks, particularly in high-density hospital environments. For Zigbee, security limitations linked to key reuse and weak join procedures were documented in [16]. Similarly, Noura et al. [17] investigated LoRaWAN's dependence on MAC-layer encryption and static key management, showing that such practices leave devices vulnerable to replay and injection attacks.

Beyond individual protocols, researchers have explored system-level risk modeling and holistic threat taxonomies. Alsubaei et al. [18] proposed a multi-layered IoMT threat taxonomy spanning hardware, software, and network domains, though the analysis remained primarily device-centric. Tournier et al. [19] introduced a unified framework for assessing IoT communication protocols by comparing heterogeneity, openness, interoperability, and security mechanisms. Their study classifies attacks at packet, protocol, and system levels, offering valuable insights into recurring weaknesses in communication stacks.

More recent contributions focus on comprehensive security governance and risk management. Svandova and Smutny [20] conducted a scoping review of IoMT risk-assessment frameworks, identifying a lack of integrated tools that address both technological and organizational aspects of healthcare cybersecurity. Dzamesi and Elsayed [21] reviewed major attack vectors such as malware propagation and distributed denial-of-service (DDoS) and advocated lightweight, standardized defenses for constrained medical devices. Asif et al. [22] proposed a two-phase dual-authentication mechanism aimed at strengthening protocol-level access control, while maintaining energy efficiency.

3. Communication protocols in IoMT

Communication protocols form the foundation of IoMT systems, enabling secure and real-time data transmission among sensing nodes, medical actuators, aggregation gateways, and cloud-based services. These protocols directly influence system latency, energy efficiency, and overall reliability while also determining the security posture of clinical data exchange [4]. Their design must therefore support mission-critical communication under stringent reliability and safety requirements, accommodating devices that range from ultra-low-power wearables to high-bandwidth diagnostic systems. Unlike general IoT environments, communication failures in IoMT deployments can directly compromise patient safety or therapeutic accuracy, making confidentiality, integrity, and availability both clinical and technical imperatives.

IoMT deployments operate across diverse environments such as hospitals, ambulatory services, assisted-living facilities, and patient homes, each imposing distinct communication constraints. In hospital networks, abundant power and infrastructure support high-bandwidth technologies, such as Wi-Fi, enabling continuous telemetry and imaging applications. In contrast, home-care and remote-monitoring systems favor low-power and low-maintenance protocols such as BLE and LoRaWAN, which balance connectivity requirements with energy efficiency [13]. These differences illustrate that communication design in IoMT is inherently context dependent, requiring trade-offs among throughput, power consumption, and regulatory compliance. In particular:

- **Bluetooth Low Energy (BLE)** is commonly embedded in wearable health trackers, glucose monitors, and portable electrocardiogram (ECG) sensors. Its low-power profile supports continuous, on-body telemetry but exposes devices to pairing and downgrade attacks if not configured with authenticated modes.
- **Zigbee** is favored in mesh-based patient monitoring systems deployed in hospital wards, where its topology supports synchronized vital-sign collection but may suffer from legacy join procedures and static network keys.
- **Wi-Fi (IEEE 802.11)** underpins high-bandwidth applications such as real-time imaging, telepresence, and access to electronic health record platforms. While ubiquitous in hospital infrastructure, partial WPA3 adoption leaves critical IoMT workflows exposed to credential theft and denial-of-service threats.
- **LoRaWAN** supports long-range, energy-efficient telemetry for home-care settings and rural patient monitoring (e.g., chronic disease management). Its over-the-air activation and star topology make it scalable but introduce risks when keys are reused or nonces are improperly handled.
- **Proprietary RF** communication is prevalent in implantable devices such as pacemakers, insulin pumps, and neurostimulators. These protocols optimize for ultra-low power and closed-loop control but often lack robust encryption or OTA update mechanisms, making post-deployment mitigation difficult or impossible.

Beyond their individual characteristics, many IoMT systems employ multi-protocol layering. For example, a wearable device may use BLE for local data collection, Zigbee for intra-hospital aggregation, and Wi-Fi for final transmission to cloud storage or hospital networks. Each layer introduces distinct encryption schemes, addressing mechanisms, and energy profiles. An example of this general layered communication architecture is illustrated in Fig. 1.

The diversity of communication technologies within IoMT introduces persistent challenges for interoperability, key management, and consistent policy enforcement. Cross-vendor integration, asynchronous update cycles, and heterogeneous protocol stacks compli-

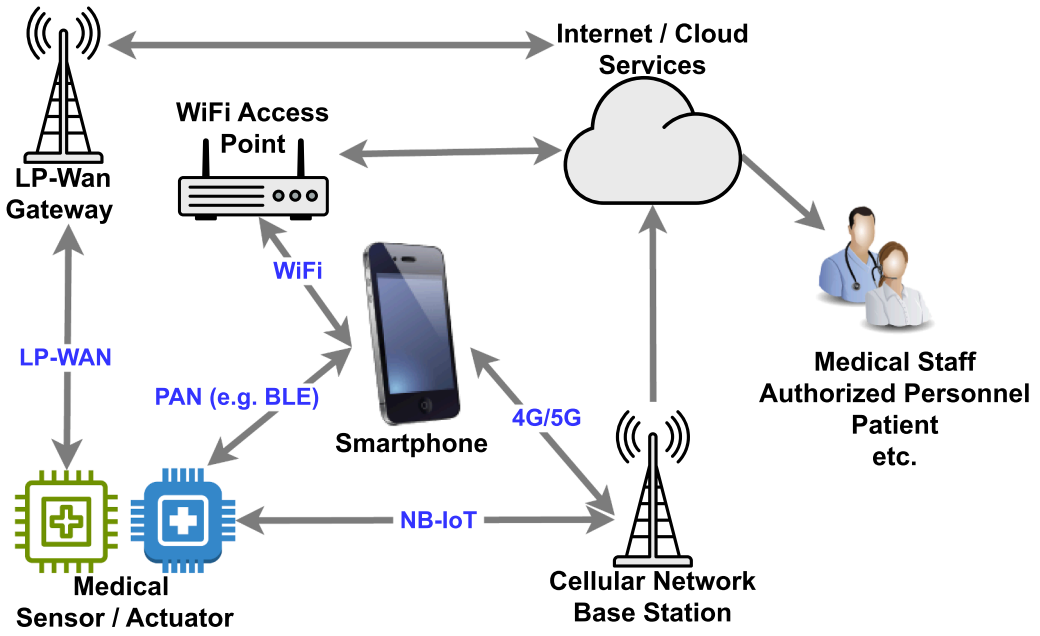

Fig. 1. Multi-protocol IoMT communication via smartphone gateway architecture.

cate unified network governance. As a result, communication layer design must be evaluated not only from a performance standpoint, but also from a security and dependability perspective.

4. Threat and vulnerability analysis

Building on the architectural overview discussed in the previous section, this section analyzes how protocol design characteristics may lead into specific vulnerabilities and cross-layer security risks, establishing the foundation for quantitative risk assessment. The IoMT threat landscape emerges from the interaction of constrained embedded devices, pervasive wireless connectivity, and heterogeneous protocol implementations, deployed across both clinical and non-clinical contexts. The analysis follows the STRIDE threat model [23], correlating known weaknesses with specific protocol behaviors and operational settings. The objective is to demonstrate how classical IoT threats emerge in safety-critical medical systems, where data integrity, device availability, and patient safety are tightly interdependent.

4.1. Threat categorization using STRIDE

The STRIDE model classifies security threats into six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege [24]. These categories are directly relevant to IoMT networks, which integrate diverse communication stacks operating under strict resource and timing constraints. Each IoMT communication protocol exhibits distinct weaknesses shaped by its design objectives, legacy compatibility, and deployment environment.

Bluetooth Low Energy (BLE) remains susceptible to inconsistencies in pairing models, optional encryption, and downgrade attacks. Devices configured with *Just Works* or *Legacy Pairing* modes are particularly exposed [18,25,26]. In clinical settings, these vulnerabilities can enable unauthorized device synchronization or falsified sensor data injection.

Legacy Zigbee deployments often rely on static pre-shared keys and insecure joining procedures. Empirical studies confirm the feasibility of replay, key extraction, and command injection attacks in operational networks [16,19]. Within hospitals, these weaknesses can compromise distributed monitoring clusters or allow unauthorized reconfiguration of network nodes.

Wi-Fi continues to represent a prominent attack vector due to its ubiquity in healthcare infrastructure. Although WPA3 enhances encryption and mutual authentication, many clinical networks still employ WPA2, leaving them susceptible to credential-based or denial-of-service attacks [15]. Since Wi-Fi underpins hospital information systems, exploitation at this layer can cascade across dependent IoMT services.

LoRaWAN provides message integrity code (MIC) protection and end-to-end payload encryption [27], yet weaknesses in device activation, frame-counter handling, and static session keys enable replay or spoofing attacks [17]. In large scale telemetry systems, such issues can result in data injection or synchronization failures.

Proprietary RF protocols, commonly employed in implantable or vendor-specific devices, frequently lack mutual authentication and robust encryption. Reverse engineering analyses reveal unencrypted telemetry, fixed keys, and command injection vectors [28].

Table 1
STRIDE threat classification in IoMT environments.

Threat Type	Representative Example in IoMT Context
Spoofing	Impersonation of legitimate sensors or gateways to inject falsified patient data
Tampering	Modification of physiological data (e.g., heart rate, glucose levels) during transmission
Repudiation	Lack of audit trails in remote monitoring sessions, enabling denial of performed actions
Information Disclosure	Passive eavesdropping on wireless links to extract sensitive health information
Denial of Service	Jamming or flooding of Zigbee/Wi-Fi channels that disrupt telemetry transmission
Elevation of Privilege	Exploitation of firmware flaws to gain unauthorized control of medical devices

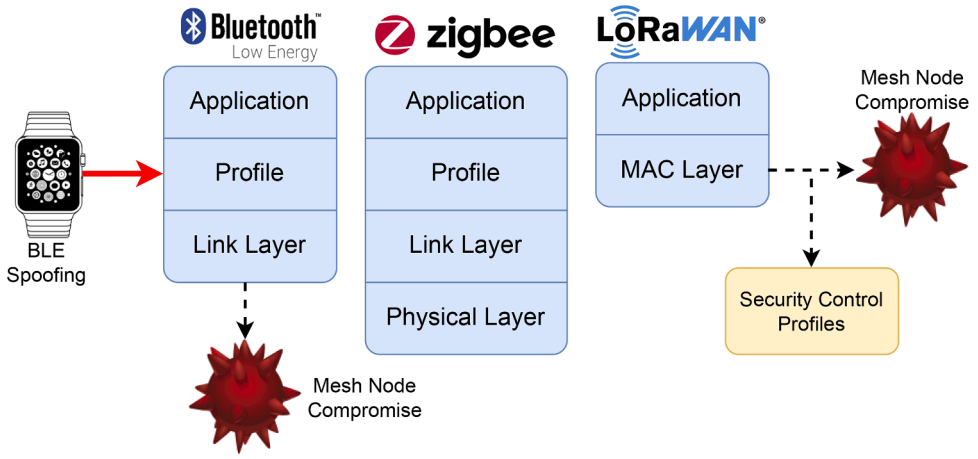

Fig. 2. IoMT security and control profiles across communication layers.

Because firmware updates are limited or infeasible in implanted systems, such vulnerabilities introduce persistent and high-impact safety risks. A notable case is the 2011–2018 Medtronic MiniMed insulin pump vulnerability, which allowed unauthenticated wireless commands to modify insulin dosage [29]. Table 1 outlines the threat categories and their typical occurrences in IoMT environments.

4.2. Cross-layer and multi-vector threats

Real-world IoMT systems typically employ multiple wireless protocols across the communication stack. While this layering enhances interoperability, it simultaneously broadens the attack surface and enables multi-vector exploitation. An adversary may compromise a wearable through BLE, pivot through a Zigbee mesh, and ultimately access backend systems over Wi-Fi. Inconsistent key-management or authentication mechanisms across these layers further facilitate replay, spoofing, or privilege-escalation attacks that traverse protocol boundaries.

Such coordinated cross-protocol attacks often bypass conventional perimeter defenses by exploiting implicit trust among interconnected components. The risk is amplified in medical environments where sensors, gateways, and backend servers operate under heterogeneous firmware versions and asynchronous patch cycles. Fig. 2 illustrates how security controls and threat exposure vary across communication layers.

Context significantly influences the threat surface. In hospitals, Wi-Fi and Zigbee networks are prone to interference and jamming under high radio-frequency density [30]. Conversely, home-based systems using BLE or LoRaWAN often lack intrusion detection or secure provisioning, exposing them to spoofing and replay attacks [31]. Implantable devices employing proprietary RF protocols remain consistently exposed to threats, mainly due to their closed nature and the inability to implement secure over-the-air (OTA) updates.

Inter-protocol dependencies within multiprotocol gateways or translation hubs present an additional challenge. These devices facilitate cross-technology communication but can propagate attacks when protections are inconsistently enforced. A breach at one interface, such as Zigbee MAC spoofing, may compromise other interfaces through shared credentials or unsynchronized encryption states [19,32]. Empirical findings confirm that fragmented authentication and asynchronous patching across stacked protocols significantly increase susceptibility to lateral movement and systemic compromise. Within clinical settings, the impact can include loss of telemetry, alert delays, or interference with therapeutic operations.

4.3. Observed risk patterns

Across IoMT communication protocols, several recurring vulnerabilities are observed. Some notable examples are the following:

- Weak or optional encryption, exposing telemetry to interception or modification.

- Absence of mutual authentication in mesh or peer-to-peer configurations, enabling spoofing and data injection.
- Insecure firmware-update and key-storage mechanisms, allowing persistent compromise.
- Limited runtime anomaly detection in constrained devices, delaying threat identification.
- High susceptibility to cross-layer exploitation in heterogeneous stacks lacking synchronized enforcement.

These weaknesses are unevenly mitigated across vendors, resulting in inconsistent security baselines throughout healthcare networks. This heterogeneity complicates unified risk modeling and limits the effectiveness of systemic security governance. The subsequent section introduces a structured, data-driven methodology to quantify these risks through a reproducible "Likelihood-Impact" framework that evaluates their relative exploitability, impact severity, and deployment context within IoMT environments.

5. Data-driven risk assessment methodology

Given the safety-critical context of IoMT ecosystems, security evaluation should distinguish technical vulnerability evidence from deployment-specific clinical and operational considerations. This section applies a normalized Exploitability–Impact formulation for comparative assessment across IoMT communication technologies. The empirical baseline is derived from CVSS v3.x data, while deployment exposure is examined separately through the scenario analysis presented in Section 6.5.

5.1. Risk quantification framework

The proposed framework provides a quantitative yet interpretable basis for the comparative assessment of protocol-associated vulnerability evidence. NIST SP 800-30 Rev. 1 describes risk as a function of likelihood and impact while allowing assessment-specific qualitative, semi-quantitative, or quantitative models [33]. Drawing only on this general likelihood–impact relationship, the present study operationally defines a study-specific comparative index as the product of normalized Exploitability and Impact proxies, where the overall risk(R) is therefore modeled as the product of two principal dimensions, Likelihood (L) and Impact (R), which jointly capture technical exploitability and the potential operational consequences of a security event:

$$R = L \times I \tag{1}$$

This formulation is not an implementation of the NIST risk tables or a NIST-calibrated risk measure. It is a continuous, dimensionless index intended solely for relative comparison of the protocol-associated vulnerability records contained in the analyzed sample. The components are defined as follows:

- **Likelihood (L)** is a normalized proxy for protocol-level exploitability derived from the mean CVSS v3.x Exploitability subscore. The symbol L is retained for consistency with the conventional Likelihood–Impact notation, but it should not be interpreted as an empirical probability of exploitation.
- **Impact (I)** is a normalized proxy for the severity of the reported vulnerabilities, derived from the mean CVSS v3.x Impact subscore. It reflects the confidentiality, integrity, and availability consequences represented in CVSS and does not directly quantify patient harm or clinical outcomes.

Both parameters are represented as continuous dimensionless indices on an approximately 0–1 comparative scale. No fixed ordinal risk categories are assigned to the resulting values. The normalized formulation is expressed as:

$$\begin{aligned} L &= \frac{E_{\text{avg}}}{E_{\max}}, \\ I &= \frac{S_{\text{avg}}}{S_{\max}}, \\ R &= L \times I, \end{aligned} \tag{2}$$

where E_{avg} and S_{avg} denote the mean CVSS v3.x Exploitability and Impact subscores, respectively, for each protocol family. The constants $E_{\max} = 3.887$ and $S_{\max} = 6.048$ are three-decimal approximations to the maximum attainable unrounded CVSS v3.x Exploitability and Impact subscores, respectively, over the permitted Base-metric combinations [34]. Their mathematical derivation is provided in Appendix B.

Higher values of R indicate greater relative composite exploitability–impact within the analyzed dataset, whereas lower values indicate lower relative values under the same normalization. No absolute Low, Moderate, or High classification, and no clinical meaning, is assigned to any particular numerical value of R. Deployment exposure is intentionally excluded from the baseline formulation in Eq. (2). This separation prevents analyst-dependent environmental assumptions from being embedded in the empirical protocol comparison. Deployment conditions are examined independently through the scenario-specific multiplier F_s introduced in Section 6.5. Consequently, Table 2 represents a common data-derived baseline against which alternative deployment scenarios may be explored.

Normalization and uncertainty assessment: Independent normalization by the theoretical CVSS subscore maxima avoids analyst-selected thresholds and accounts for the different ranges of the Exploitability and Impact subscores. Because the normalization constants are derived from theoretical maxima rather than from analyst-selected category boundaries, no threshold calibration is required. Uncertainty in the protocol-level estimates is assessed in Section 5.4 through bootstrap confidence intervals and non-parametric distribution-level statistical analysis.

5.2. Data collection and processing pipeline

To operationalize the proposed model, vulnerability data were collected from the National Vulnerability Database (NVD)[2] using the six NVD JSON 2.0 year feeds labelled 2020 through 2025. These feeds are organized according to the year component of the CVE identifier. Accordingly, the study window refers to the selected NVD year feeds rather than necessarily to CVE publication dates. Because historical NVD records may subsequently be modified, the retrieval date defines the data snapshot analyzed in this study. The NVD was selected because it provides an authoritative and structured representation of Common Vulnerabilities and Exposures (CVEs), including standardized CVSS v3.x scoring fields. This enables reproducible and quantitatively grounded parameter estimation for each protocol family.

The NVD feeds were downloaded as compressed files. The collection and processing workflow was implemented in Python using the standard `json` library and consisted of four stages:

1. **Acquisition:** The six NVD JSON 2.0 year feeds labelled 2020 through 2025 were processed. Each record contains the CVE identifier, textual vulnerability description, references, and structured CVSS v3.x metrics used in the subsequent empirical analysis.
2. **Filtering:** Keyword-based pattern matching was applied to identify CVEs associated with communication protocols commonly used in IoMT systems. The search set included protocol names and related technical terms such as *Bluetooth*, *BLE*, *Zigbee*, *Wi-Fi*, *802.11*, *WPA2*, *WPA3*, and *LoRaWAN*. Case-insensitive regular-expression matching was used to capture naming variations across records (e.g., “BLE” and “802.11”).
3. **Deduplication and protocol relevance screening:** Duplicate CVE entries and alias identifiers were removed using the CVE-ID key. Protocol relevance was determined from the textual vulnerability descriptions and reference information using protocol-specific keyword patterns. Records with missing or inconsistent CVSS v3.x Exploitability or Impact subscores were excluded from the quantitative analysis.
4. **Computation:** For each protocol subset, the mean Exploitability and Impact subscores (E_{avg}, S_{avg}) were computed, followed by normalized Likelihood and Impact indices (L, I) and their composite risk index ($R = L \times I$) according to Eq. (2).

The process was automated through a reproducible Python pipeline to ensure consistency across yearly updates. The pseudocode of the data-processing algorithm is shown in Algorithm 1.

Algorithm 1 Protocol-specific CVE extraction and scoring pipeline.

Input: NVD JSON 2.0 year feeds labelled 2020–2025
Output: Structured protocol-level CVE table with CVSS-derived risk parameters
Merge the six NVD JSON 2.0 year feeds
Initialize empty protocol-specific subsets and an empty set of processed CVE identifiers
for each CVE record **do**
    if the CVE identifier has not previously been processed **then**
        Add the CVE identifier to the set of processed identifiers
        Apply the protocol-specific keyword filters
        Screen for protocol relevance and validate the CVSS v3.x fields
        if the record matches one or more protocol patterns and contains valid Exploitability (E) and Impact (S) subscores **then**
            Store E and S in each corresponding protocol subset
        end if
    end if
end for
for each protocol subset p **do**
    Compute $E_{\text{avg},p}$ and $S_{\text{avg},p}$
    Compute $L_p = E_{\text{avg},p}/E_{\max}$, $I_p = S_{\text{avg},p}/S_{\max}$, and $R_p = L_p \times I_p$
end for

A total of 4378 protocol-related CVE records with valid CVSS v3.x Exploitability and Impact subscores were retained across the five communication protocol families. Bluetooth and Wi-Fi dominate the resulting dataset, with 2767 and 1472 retained CVEs, respectively, whereas Zigbee, LoRaWAN, and proprietary RF contain substantially smaller subsets. This imbalance is explicitly considered in the subsequent statistical and uncertainty analyses.

It should be noted that the resulting dataset is *protocol-oriented* rather than exclusively medical device specific. In other words, not every retained CVE corresponds to a deployed medical product. Instead, the dataset captures vulnerabilities affecting communication technologies that are also used within IoMT systems. For this reason, the analysis should be interpreted as a comparative assessment of protocol-level security exposure relevant to IoMT communication stacks, rather than as a direct enumeration of clinical-device incidents.

[2] The NVD JSON 2.0 year feeds labelled 2020 through 2025 were retrieved on 19 August 2026.

Table 2
Empirical CVSS statistics and normalized composite indices for the protocol-oriented sample derived from the NVD year feeds labelled 2020–2025.

Protocol	CVE Count	E_{avg}	S_{avg}	L	I	R
Bluetooth	2767	2.383	3.983	0.613	0.659	0.404
Zigbee	15	3.147	4.200	0.810	0.694	0.562
Wi-Fi	1472	2.397	4.650	0.617	0.769	0.474
LoRaWAN	14	2.386	3.721	0.614	0.615	0.378
Proprietary RF	110	2.541	4.167	0.654	0.689	0.450

Table 3
Descriptive statistics and bootstrap uncertainty estimates for CVSS Exploitability, Impact, and the normalized composite index across protocol families.

Protocol	n	E_{mean}	E_{median}	E_{IQR}	S_{mean}	S_{median}	S_{IQR}	R	95% CI for R
Bluetooth	2767	2.383	2.30	1.00	3.983	3.60	2.50	0.404	[0.396, 0.411]
Zigbee	15	3.147	3.90	1.60	4.200	3.60	1.35	0.562	[0.484, 0.629]
Wi-Fi	1472	2.397	2.20	1.00	4.650	5.20	2.30	0.474	[0.462, 0.486]
LoRaWAN	14	2.386	2.55	1.075	3.721	3.50	3.10	0.378	[0.279, 0.487]
Proprietary RF	110	2.541	2.30	2.10	4.167	4.00	2.30	0.450	[0.407, 0.495]

5.3. Empirical CVSS-based metrics

For each protocol, the mean CVSS Exploitability (E_{avg}) and Impact (S_{avg}) subscores were normalized by their respective theoretical CVSS maxima, $E_{max} = 3.887$ and $S_{max} = 6.048$, placing both dimensions on a common approximately 0–1 comparative scale.

Table 2 summarizes the resulting Likelihood, Impact, and composite risk indices across protocols. These values are intended for relative comparison under the normalization scheme introduced in Section 5, rather than as absolute measures of real-world clinical risk.

The normalized point estimates remain within a relatively narrow comparative range, with Zigbee showing the highest composite value ($R = 0.562$), followed by Wi-Fi ($R = 0.474$), proprietary RF ($R = 0.450$), Bluetooth ($R = 0.404$), and LoRaWAN ($R = 0.378$). However, these point estimates should not be interpreted as absolute risk levels or as direct evidence that one protocol is intrinsically more vulnerable than another. The protocol subsets differ substantially in sample size, particularly for Zigbee and LoRaWAN, and therefore the uncertainty associated with their estimates is considerably greater. For this reason, the protocol-level averages are complemented below by distribution-level statistical testing and bootstrap uncertainty analysis.

5.4. Statistical analysis of cross-protocol differences

To determine whether the observed protocol-level differences extend beyond comparison of mean CVSS values, the individual CVE Exploitability (E) and Impact (S) observations were subjected to distribution-level statistical analysis. Given the strongly unequal sample sizes among protocol families and the bounded nature of CVSS subscores, a non-parametric statistical approach was adopted without assuming normality.

For each protocol, the mean, median, and interquartile range (IQR) were calculated for the Exploitability and Impact subscores. In addition, bootstrap resampling with 10,000 iterations was used to estimate 95% confidence intervals for the protocol-level composite risk index R.

Cross-protocol differences were assessed using the Kruskal–Wallis rank-based non-parametric test [8]. To complement the omnibus significance tests, the corresponding effect size was calculated as ordinal eta-squared based on the Kruskal–Wallis statistic:

$$\eta_H^2 = \frac{H - k + 1}{N - k},$$

where H is the Kruskal–Wallis test statistic, k is the number of protocol groups, and N is the total number of observations [9,10].

For Exploitability, the omnibus test produced $H(4) = 9.210$ and $p = .0561$, indicating that the differences in Exploitability distributions across the five protocol families do not reach the conventional 0.05 significance threshold. The corresponding effect size was negligible ($\eta_H^2 \approx 0.0012$). Therefore, the higher Exploitability point estimate observed for Zigbee should not be interpreted as statistically established evidence of greater exploitability.

For Impact, the Kruskal–Wallis test identified a statistically significant cross-protocol difference, with $H(4) = 255.983$ and $p < .001$. The corresponding effect size was $\eta_H^2 \approx 0.058$, indicating a measurable but modest protocol-related difference in the Impact distributions. Because the omnibus Impact test was statistically significant, pairwise post-hoc comparisons were conducted using Dunn's rank-sum procedure [11], with Holm's sequential correction applied to control the family-wise error rate [12]. These comparisons showed that Wi-Fi exhibited significantly higher Impact scores than Bluetooth ($p_{Holm} < 0.001$) and proprietary RF ($p_{Holm} = 0.0156$). Other pairwise differences did not remain statistically significant after correction for multiple comparisons.

The statistical results therefore show that the most robust cross-protocol distinction in the dataset concerns Impact rather than Exploitability. In particular, Wi-Fi combines a large vulnerability population with a comparatively elevated Impact distribution,

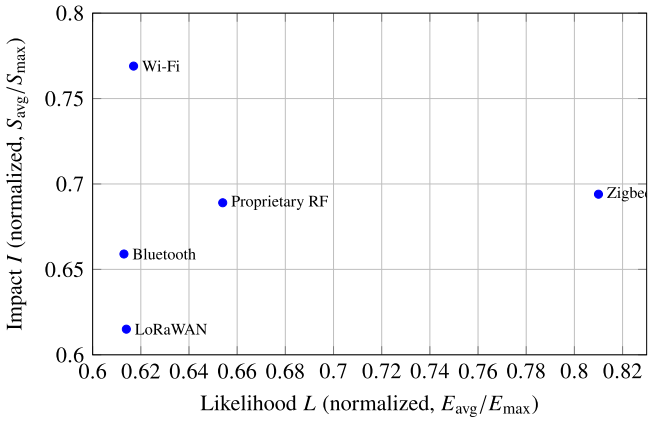

Fig. 3. Empirical normalized Likelihood–Impact distribution by protocol for the protocol-oriented sample derived from the NVD JSON 2.0 year feeds labelled 2020–2025, with Exploitability and Impact normalized by their respective theoretical CVSS subscore maxima.

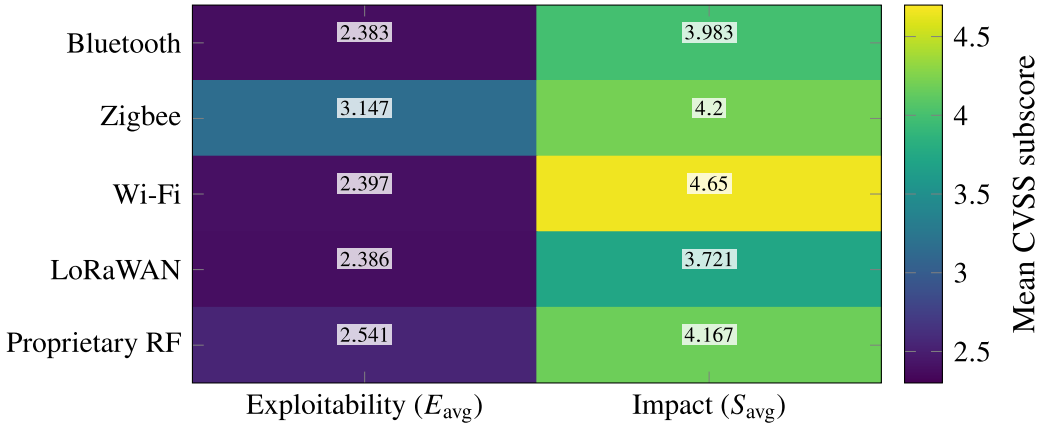

Fig. 4. Comparative heatmap of mean CVSS v3.x Exploitability and Impact subscores by protocol for the protocol-oriented sample derived from the NVD JSON 2.0 year feeds labelled 2020–2025. Cells report the corresponding mean subscores. Comparisons should be made within each column because Exploitability and Impact have different theoretical maxima.

whereas the high Zigbee point estimate is associated with substantially greater uncertainty because of the limited number of retained CVEs.

Table 3 reports the corresponding descriptive statistics and bootstrap confidence intervals.

Fig. 3 illustrates the normalized Likelihood–Impact distribution derived from the protocol-oriented sample obtained from the NVD JSON 2.0 year feeds labelled 2020 through 2025. Independent normalization of the two CVSS dimensions places Exploitability and Impact on a common scale while preserving their different cross-protocol patterns. Wi-Fi exhibits the highest normalized Impact value, whereas Zigbee exhibits the highest normalized Exploitability point estimate. As demonstrated by the statistical analysis, however, only the cross-protocol differences in Impact are statistically significant.

Fig. 4 complements the normalized comparison by reporting the corresponding mean unnormalized CVSS Exploitability and Impact subscores.

The normalized composite indices occupy a relatively narrow range ($R \in [0.378, 0.562]$), reflecting the comparative nature of the baseline formulation. Deployment conditions are excluded from these baseline values and are introduced only through the scenario-specific multiplier F_s defined in Section 6.5. Under the illustrative higher-exposure scenario ($F_s = 1.5$), the scenario-adjusted indices range from approximately 0.57 to 0.84, whereas under the illustrative lower-exposure scenario ($F_s = 0.75$), they range from approximately 0.28 to 0.42. Because the same multiplier is applied to every protocol, the relative ordering remains unchanged. These values represent sensitivity to explicitly specified what-if assumptions and should not be interpreted as measured differences between hospital and home-care deployments.

Protocols with limited updateability or constrained post-deployment hardening options, especially proprietary RF in implantable or telemetry devices, may still require compensating controls such as encrypted encapsulation, electromagnetic shielding, or anomaly-based monitoring to support operational safety. No fixed numerical value of R is interpreted as clinically acceptable, manageable, or unacceptable. The index is used solely for relative cross-protocol comparison; operational acceptability requires a device- and deployment-specific cybersecurity and safety assessment.

Clinical and Regulatory Relevance: The scenario analysis illustrates how a common empirical protocol baseline may acquire greater operational significance under increased deployment exposure. Under the illustrative higher-exposure hospital scenario ($F_s = 1.5$), the scenario-adjusted indices are approximately $R_s = 0.606$ for BLE, $R_s = 0.843$ for Zigbee, $R_s = 0.711$ for Wi-Fi, $R_s = 0.566$ for LoRaWAN, and $R_s = 0.676$ for proprietary RF. These values are comparative what-if indices rather than clinically calibrated risk estimates. Their purpose is to support consideration of protocol choice, deployment context, and security configuration when prioritizing communication-layer safeguards. They do not establish risk acceptability thresholds or quantify patient risk.

6. Mitigation strategies

Securing IoMT communication requires a layered and context-aware approach in which protocol-specific weaknesses and system-level risks are jointly addressed. The following strategies, derived from structured threat modeling and empirical findings, are applied across device, network, and application layers while considering the operational environment.

6.1. Device-level mitigations

At the device layer, foundations of trust and updateability must be strengthened. Where feasible, hardware roots of trust such as Trusted Platform Modules [35] or Secure Elements [36] must be integrated to enable secure boot, key protection, and tamper evidence. For legacy or constrained devices, lightweight firmware hardening and authenticated bootloaders should be applied. Signed firmware and pre-execution validation are required in regulated environments to ensure integrity. Energy-efficient cryptographic primitives, such as elliptic curve cryptography (ECC), should be preferred, and session-based or rolling keys should be used where full mutual authentication cannot be supported. Authenticated over-the-air (OTA) update channels (e.g., TUF [37]) must be established to provide resilience throughout the post-market phase.

6.2. Network and communication stack mitigations

At the network and protocol layers, strong default configurations must be enforced and medical traffic must be isolated. For BLE and Zigbee, secure pairing methods (Numeric Comparison or Passkey) and AES-128 link encryption must be required, while legacy join modes and static keys must be disabled. For Wi-Fi, WPA3 should be adopted, IoMT traffic should be segmented (e.g., through VLANs), and lateral movement should be restricted by means of policy gateways and firewalls. RF and flow aware intrusion detection systems must be deployed to detect jamming or flooding attempts in dense clinical environments. For LoRaWAN, MAC-layer protections must be complemented with application-layer encryption. Over-The-Air-Activation (OTAA) should be preferred, frame counters must be enforced, and session keys must be periodically rotated. Gateways must verify the authenticity and integrity of relayed packets to prevent manipulation at intermediate nodes.

6.3. Application and system level measures

End-to-end encryption must be enforced between the device and the hospital information system or cloud service, regardless of intermediate protocol protections. Mutual authentication using certificates or hardware-bound tokens must be applied during device onboarding and access authorization. Application programming interfaces must be hardened through rate limiting, input validation, and anomaly detection to prevent brute-force or data-exfiltration attempts. Supply-chain protection frameworks such as TUF must be adopted to safeguard update integrity, while audit-grade logging must be maintained to support regulatory traceability and forensic readiness. Application-layer allowlists and behavioral baselines should be implemented to detect misuse, even when lower communication layers are compromised.

6.4. Deployment-aware strategies

Mitigation measures must be adapted to the operational environment, since the same protocol may present different exposure characteristics across hospital, home-care, and implantable-device settings. In hospital infrastructures, logically segmented medical networks, WPA3 isolation, centralized key management, and continuous monitoring are recommended in order to limit lateral movement and reduce the effects of dense wireless coexistence. Integrations with electronic health record (EHR) systems should additionally enforce role-based access control and periodic credential rotation. In home or ambulatory deployments, self-configuring onboarding, automated updates, and lightweight anomaly detection or remote attestation can help identify compromised nodes without imposing excessive monitoring overhead. In implantable or highly constrained environments, where updateability may be limited, compensating controls such as shielding, secure telemetry encapsulation, and conservative communication configurations become especially important. In all cases, protection mechanisms must be balanced with usability, maintainability, and clinical feasibility throughout the device lifecycle.

6.5. Scenario-based sensitivity analysis

To examine how explicitly specified deployment assumptions affect the common empirical baseline, the composite index is extended through a scenario-specific multiplier F_s. For each deployment context, the scenario-adjusted comparative index R_s is defined

Table 4
Illustrative scenario-adjusted comparative indices, mitigation measures, and residual-risk considerations for IoMT communication protocols.

Protocol	Threats and risk impact	Scenario-adjusted index	Mitigation measures	Residual-risk considerations
Bluetooth Low Energy (BLE)	Spoofing, sniffing, and downgrade attacks through insecure pairing threaten telemetry confidentiality and device integrity.	$R_s \approx 0.606$ (hospital, $F_s = 1.5$) $R_s \approx 0.404$ (mixed, $F_s = 1.0$)	LE Secure Connections, authenticated pairing, disabling "Just Works," periodic key rotation, and signed OTA updates.	Authenticated pairing and signature validation can reduce MitM and firmware-abuse exposure; residual risk remains for legacy BLE 4.x devices and inconsistent implementation settings.
Zigbee	Replay and spoofed-node injection exploiting weak join and static keys can compromise entire mesh clusters.	$R_s \approx 0.843$ (hospital, $F_s = 1.5$) $R_s \approx 0.562$ (mixed, $F_s = 1.0$)	Install codes, link-key refresh, OTA revocation, and secure gateway bridging with intrusion detection.	Controlled joins and improved key management can reduce lateral propagation, although residual risk remains sensitive to heterogeneous firmware and legacy deployment practices.
Wi-Fi	Credential theft, deauthentication, and RF jamming may disrupt clinical telemetry or leak PHI over shared infrastructure.	$R_s \approx 0.711$ (hospital, $F_s = 1.5$) $R_s \approx 0.474$ (mixed, $F_s = 1.0$)	Migration to WPA3, VLAN segmentation, AP isolation, network firewalls, and spectral anomaly detection.	WPA3 and segmentation can reduce credential abuse and lateral pivoting, although residual exposure may persist where adoption is incomplete or interoperability constraints remain.
LoRaWAN	Replay and injection via weak activation or nonce handling reduce telemetry reliability.	$R_s \approx 0.566$ (hospital, $F_s = 1.5$) $R_s \approx 0.378$ (mixed, $F_s = 1.0$)	OTAA activation, frame-counter enforcement, key rotation, and end-to-end encryption.	OTAA, counter validation, and stronger key management can reduce replay exposure, while end-to-end encryption mitigates dependence on intermediate gateways.
Proprietary RF	Fixed keys and undocumented control channels enable unauthorized actuation or patient-data leakage.	$R_s \approx 0.676$ (hospital, $F_s = 1.5$) $R_s \approx 0.450$ (mixed, $F_s = 1.0$)	Protocol hardening, shielding, cryptographic encapsulation, anomaly detection, and post-market update pathways.	Security wrapping and anomaly monitoring can partially compensate for the lack of OTA support; however, residual risk may remain elevated in non-upgradable legacy implants and opaque vendor implementations.

Note: $R_s = R \times F_s$ reflects an explicitly specified deployment scenario and does not alter the empirical baseline in Table 2. The hospital and mixed values are illustrative what-if indices rather than measured deployment risk. Numerical post-mitigation indices are not reported because control effectiveness was not calibrated using implementation-specific or operational healthcare data.

as:

$$R_s = R \times F_s = L \times I \times F_s. \tag{3}$$

Here, F_s is a dimensionless scenario multiplier applied only after the baseline index R has been calculated. In this study, $F_s = 1.0$ represents a mixed or baseline exposure setting, $F_s = 1.5$ represents an illustrative higher-exposure hospital setting, and $F_s = 0.75$ represents an illustrative lower-exposure home-care or isolated setting. These values are specified solely for what-if sensitivity analysis and are not coefficients estimated or calibrated from operational healthcare data. Because the same F_s is applied to every protocol within a scenario, it changes the magnitude of R_s but does not change the empirical baseline or the protocol ordering reported in Table 2.

Like R, the scenario-adjusted quantity R_s is a dimensionless comparative index. It is not a probability, a clinically calibrated risk measure, or a direct empirical measurement of hospital or home-care risk. No numerical value of R_s is interpreted as an acceptable, manageable, or unacceptable risk threshold.

The effectiveness of the listed mitigation controls was not estimated using an independent validation dataset or measured deployment outcomes. Numerical post-mitigation risk values are therefore not reported. Table 4 instead presents protocol-specific mitigation measures and qualitative residual-risk considerations. Quantitative residual-risk estimation would require implementation-specific evidence concerning control effectiveness, configuration, asset criticality, and operational exposure.

7. Discussion

7.1. Cross-protocol interpretation of empirical results

The empirical results reveal substantial differences in vulnerability volume, severity distribution, and uncertainty across the five protocol families, but these dimensions should not be interpreted interchangeably. Bluetooth contains the largest retained vul-

nerability population ($n = 2767$), followed by Wi-Fi ($n = 1472$), proprietary RF ($n = 110$), Zigbee ($n = 15$), and LoRaWAN ($n = 14$). However, vulnerability frequency alone does not determine the severity of the protocol-level profile. Bluetooth, for example, exhibits $E_{avg} = 2.383$ and $S_{avg} = 3.983$, resulting in $R = 0.404$, despite accounting for the majority of the retained CVEs. Its large CVE population is consistent with the breadth of the Bluetooth ecosystem and the diversity of implementations, pairing modes, and legacy compatibility mechanisms reported in the literature [18,25,26]. The result therefore illustrates why vulnerability counts should not be treated as direct proxies for security risk.

Zigbee has the highest Exploitability point estimate ($E_{avg} = 3.147$) and the highest baseline composite index ($R = 0.562$), with $S_{avg} = 4.200$. This profile is consistent with security concerns associated with weak joining procedures, static or reused keys, and the possibility that compromise of one node may propagate through a mesh topology [16,19]. Nevertheless, only 15 Zigbee CVEs were retained, and the bootstrap interval for R is correspondingly wide ([0.484, 0.629]). Moreover, the overall difference in Exploitability across protocols did not reach statistical significance ($p = .0561$). The Zigbee result should therefore be interpreted as an elevated point estimate with substantial uncertainty rather than as evidence that Zigbee is intrinsically more exploitable than the other protocol families.

Wi-Fi presents a different pattern. Its mean Exploitability ($E_{avg} = 2.397$) is close to that of Bluetooth and LoRaWAN, but its mean Impact is the highest among the five protocols ($S_{avg} = 4.650$), producing $R = 0.474$. The statistical analysis confirms that Impact, rather than Exploitability, is the more robust differentiating dimension since the overall Impact distributions differ significantly ($H(4) = 255.983$, $p < .001$), and Wi-Fi exhibits significantly higher Impact than Bluetooth and proprietary RF after Holm correction. This result is operationally plausible because Wi-Fi often supports shared infrastructure, high-bandwidth clinical services, and connectivity to broader hospital information systems; compromise, credential theft, deauthentication, or service disruption at this layer can therefore affect multiple dependent services [15,38].

LoRaWAN exhibits the lowest baseline composite point estimate ($E_{avg} = 2.386$, $S_{avg} = 3.721$, $R = 0.378$). However, the small number of retained observations ($n = 14$) produces the widest bootstrap interval for R ([0.279, 0.487]). The lower point estimate should therefore not be interpreted as evidence that LoRaWAN is intrinsically secure. Weaknesses associated with activation procedures, nonce handling, frame counters, and key management remain relevant, particularly in remotely managed deployments [17,27]. The result instead highlights the need to distinguish lower observed NVD severity from absence of attack surface.

Proprietary RF occupies an intermediate position ($E_{avg} = 2.541$, $S_{avg} = 4.167$, $R = 0.450$). Unlike widely standardized protocols, proprietary RF implementations may have smaller publicly visible vulnerability populations, while closed designs, fixed keys, limited updateability, and restricted implementation transparency can make individual weaknesses operationally persistent [28,29]. Consequently, a smaller CVE population should not automatically be interpreted as a smaller underlying attack surface. This distinction is particularly important for implantable or long-lived medical devices, where remediation may be constrained after deployment.

The scenario analysis reinforces the distinction between intrinsic vulnerability evidence and deployment exposure. Applying the common higher-exposure hospital multiplier ($F_s = 1.5$) produces $R_s \approx 0.606$, 0.843, 0.711, 0.566, and 0.676 for BLE, Zigbee, Wi-Fi, LoRaWAN, and proprietary RF, respectively. Because the same multiplier is applied to each empirical baseline, the relative ordering is preserved, while the magnitude of the comparative index increases. These values do not constitute measured hospital risk. Rather, they demonstrate how deployment assumptions can amplify an empirically derived protocol baseline without being embedded in the baseline itself.

7.2. Practical implications for IoMT security

The results have several implications for vulnerability management in IoMT environments. First, prioritization should not be based on CVE counts alone. Bluetooth has by far the largest number of retained vulnerabilities but a lower mean composite index than Zigbee, Wi-Fi, and proprietary RF. Conversely, Wi-Fi does not have the highest Exploitability score but exhibits the strongest Impact distribution. Vulnerability-management programs should therefore combine vulnerability prevalence with severity, device criticality, network dependence, and the feasibility of remediation.

For Wi-Fi-based medical systems, the elevated Impact profile supports particular attention to timely patching, WPA3 migration where feasible, network segmentation, access-point isolation, credential protection, and monitoring for deauthentication or jamming. For BLE, the very large vulnerability population emphasizes asset inventory, secure pairing configuration, disabling legacy or unauthenticated modes where possible, key management, and signed firmware updates. Zigbee deployments require controlled joining, strong link-key management, gateway protection, and monitoring for compromise propagation through mesh nodes. LoRaWAN deployments should prioritize secure activation, frame-counter enforcement, nonce management, key rotation, and physical protection of gateways. Proprietary RF systems require particular attention to compensating controls, because cryptographic redesign or firmware remediation may not be possible in already deployed or implantable devices.

These findings are also relevant beyond individual protocols. IoMT systems frequently combine several communication technologies through gateways and backend services. A weakness with comparatively limited local consequences can therefore become more significant when it enables lateral movement into a higher-impact communication layer. Vulnerability management should consequently consider protocol dependencies, gateway trust relationships, patch synchronization, and shared infrastructure rather than assessing each wireless interface in isolation. From a procurement and lifecycle perspective, updateability, secure provisioning, key-management capability, monitoring support, and vendor vulnerability-response processes should be evaluated alongside communication performance and energy requirements.

Finally, the separation between the empirical baseline and F_s provides a practical way to distinguish vulnerability evidence from deployment assumptions. The baseline results can support comparative screening, while scenario analysis can be used to explore

how deployment density or operational exposure may change priorities. The resulting indices should support, rather than replace, device-specific risk assessment, clinical engineering judgement, and established cybersecurity and safety-management processes.

7.3. Uncertainty and limitations

The empirical results should be interpreted in light of several sources of uncertainty. First, the protocol subsets are strongly imbalanced. Bluetooth and Wi-Fi account for most retained records, whereas Zigbee and LoRaWAN contain only 15 and 14 CVEs, respectively. The bootstrap confidence intervals quantify part of this uncertainty, but small samples still limit the stability of protocol-level point estimates. This is especially important when interpreting the comparatively high Zigbee R value and the comparatively low LoRaWAN value.

Second, NVD observations reflect publicly disclosed vulnerabilities and therefore depend on vendor disclosure practices, product popularity, researcher attention, and the availability of CVSS information. A protocol with fewer retained CVEs cannot consequently be assumed to possess fewer undiscovered or unpublished vulnerabilities. CVSS Exploitability and Impact subscores also characterize properties of reported vulnerabilities rather than complete end-to-end clinical risk, and the protocol-oriented dataset includes technologies used both within and outside medical-device deployments.

A limitation of this study is that the empirical evidence is derived from secondary vulnerability records rather than controlled experiments on medical-device testbeds or observations from operational clinical deployments. Consequently, the reported indices characterize comparative protocol-level vulnerability exposure and should not be interpreted as direct estimates of patient-level or deployment-specific clinical risk. Physical testbed validation would require representative implementations of each protocol, comparable medical-device configurations, controlled attack scenarios, and consistent operational conditions across the five protocol families. Such external validation is beyond the scope of the present dataset-driven study and constitutes an important next step for evaluating the transferability of the observed vulnerability patterns to specific IoMT deployments.

Finally, the deployment multiplier F_s is an analytical scenario parameter rather than a coefficient calibrated from operational healthcare data. It is intentionally separated from the empirical baseline and is used solely for sensitivity and what-if analysis. Because the effectiveness of the listed mitigation controls was not estimated from deployment evidence, the study does not report numerical post-mitigation indices.

8. Conclusion and future work

As IoMT systems continue to transform healthcare through pervasive connectivity, the security of their communication infrastructures remains a fundamental challenge. This study presented a structured comparative assessment of five communication technologies relevant to IoMT, namely BLE, Zigbee, Wi-Fi, LoRaWAN, and proprietary RF. The analysis combined qualitative threat modelling with a protocol-oriented evaluation of 4378 retained NVD vulnerability records. The normalized baseline composite indices ranged from $R = 0.378$ to $R = 0.562$. Cross-protocol differences were statistically significant for Impact but not for Exploitability, highlighting the importance of considering score distributions and uncertainty rather than relying on vulnerability counts or protocol-level means alone. Deployment exposure was examined separately through explicitly specified scenario multipliers and was not treated as an empirically calibrated measure of hospital or home-care risk.

A deployment-aware mitigation perspective was also provided, tailored to the operational characteristics of medical systems. Device, network, and application-layer countermeasures were discussed alongside environment-specific considerations for hospital, home-care, and constrained-device settings. Through this approach, the study showed how protocol configuration, deployment context, and security controls must be considered together in order to support more informed protocol selection, mitigation planning, and communication-layer assurance in IoMT systems.

Future work should further strengthen automation and assurance in IoMT cybersecurity assessment. Priority should be given to the integration of security-by-design verification and automated threat-assessment tools within certification-oriented workflows. As part of the MedSecurance project, supporting tools have been designed and developed with consideration of the findings presented in this paper. Formal verification and model-checking techniques may further improve confidence in protocol behavior under adversarial conditions. In addition, context-aware security orchestration mechanisms, in which communication parameters are dynamically adapted to real-time risk indicators, represent a promising direction for future research.

AI-driven anomaly detection may also enhance communication-layer monitoring by identifying abnormal protocol behavior, suspicious traffic patterns, or deviations from expected device interaction profiles in resource-constrained healthcare environments. In this respect, recent AI-enabled approaches for adaptive optimization of healthcare-oriented IoT communications suggest that similar intelligent mechanisms could be extended beyond efficiency objectives toward security-oriented monitoring and risk-aware protocol management [39].

Finally, continued alignment with regulatory frameworks such as FDA premarket cybersecurity guidance and IEC 81001-5-1 remains important for the development of more consistent IoMT risk-assessment practices and assurance toolchains.

CRediT authorship contribution statement

Charalampos Sergiou: Writing – review & editing, Writing – original draft, Software, Methodology; **Costas Iordanou:** Writing – review & editing, Writing – original draft, Methodology; **Konstantinos Katzis:** Writing – review & editing, Writing – original draft, Methodology; **Gregory Epiphaniou:** Writing – review & editing, Writing – original draft, Methodology; **Nabil Moukafih:** Writing –

review & editing, Writing – original draft, Methodology; **Carsten Maple:** Writing – review & editing; **Nikolaos Matragkas:** Writing – review & editing; **Marcos Didonet del Fabro:** Writing – review & editing.

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process

During the preparation of this work, the author(s) made limited use of ChatGPT (GPT-5, OpenAI) to assist with minor language refinement, grammar correction, and improvement of clarity and structure in a few sections of the manuscript. After using this tool, the author(s) carefully reviewed and edited all content, and take full responsibility for the integrity and accuracy of the published article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The authors have no competing interests to declare that are relevant to the content of this article.

Acknowledgments

The research described has been carried out as part of the MedSecurance Project, which has received funding from the European Union's Horizon Europe Research and Innovation Programme under grant agreement No. 101095448.

Data availability

The datasets generated and/or analyzed during the current study are derived from publicly available sources, specifically the National Vulnerability Database (https://nvd.nist.gov/). All scripts used for data collection and analysis are available from the corresponding author upon reasonable request.

Appendix A. Mathematical specification of the statistical analysis

This appendix provides the mathematical specification of the descriptive, bootstrap, omnibus, effect-size, and post-hoc procedures used in Section 5.4. All calculations were performed using the individual retained CVE observations rather than the five protocol-level mean values. The Exploitability and Impact distributions were analyzed separately.

A.1. Data structure and notation

Let $i = 1, \dots, k$ index the $k = 5$ protocol families, ordered as Bluetooth, Zigbee, Wi-Fi, LoRaWAN, and proprietary RF. The corresponding sample sizes were

$$(n_1, n_2, n_3, n_4, n_5) = (2767, 15, 1472, 14, 110), \tag{A.1}$$

with total sample size

$$N = \sum_{i=1}^{k} n_i = 4378. \tag{A.2}$$

Each retained CVE contributed one paired observation

$$\mathbf{x}_{ij} = (E_{ij}, S_{ij}), \qquad j = 1, \dots, n_i, \tag{A.3}$$

where E_{ij} and S_{ij} are the CVSS v3.x Exploitability and Impact subscores, respectively, for observation j in protocol group i. Each CVE was assigned to a single protocol group in the statistical dataset, so that the five group counts sum to N.

The statistical procedures described below were applied separately to $X = E$ and $X = S$. Thus, the Exploitability and Impact distributions were tested independently.

A.2. Descriptive statistics

For an outcome $X \in \{E, S\}$, the protocol-level arithmetic mean was

$$\bar{X}_i = \frac{1}{n_i} \sum_{j=1}^{n_i} X_{ij}. \tag{A.4}$$

The protocol-level median was

$$\widetilde{X}_i = \text{median}\left(X_{i1}, X_{i2}, \dots, X_{in_i}\right), \tag{A.5}$$

and the interquartile range was calculated as

$$\mathrm{IQR}(X_i) = Q_{0.75}(X_i) - Q_{0.25}(X_i), \tag{A.6}$$

where $Q_p(X_i)$ denotes the empirical p-quantile of the observations belonging to protocol i.

The normalized protocol-level indices were calculated from the unrounded means as

$$L_i = \frac{\bar{E}_i}{E_{\max}}, \qquad I_i = \frac{\bar{S}_i}{S_{\max}}, \qquad R_i = L_i I_i, \tag{A.7}$$

where

$$E_{\max} = 3.887, \qquad S_{\max} = 6.048. \tag{A.8}$$

A.3. Bootstrap confidence intervals

Bootstrap resampling was used to quantify uncertainty in each protocol-level composite index R_i. Resampling was conducted separately within each protocol family using $B = 10{,}000$ iterations.

For bootstrap iteration b, a sample of n_i indices was drawn with replacement from

$$\{1, 2, \ldots, n_i\}. \tag{A.9}$$

The Exploitability and Impact values belonging to the same CVE were resampled together. This paired record-level resampling preserves the empirical dependence between the two CVSS subscores.

Let $\mathcal{J}_i^{(b)}$ denote the bootstrap index sample for protocol i. The bootstrap means were

$$\bar{E}_i^{*(b)} = \frac{1}{n_i} \sum_{j \in \mathcal{J}_i^{(b)}} E_{ij}, \tag{A.10}$$

and

$$\bar{S}_i^{*(b)} = \frac{1}{n_i} \sum_{j \in \mathcal{J}_i^{(b)}} S_{ij}. \tag{A.11}$$

The corresponding bootstrap indices were calculated as

$$L_i^{*(b)} = \frac{\bar{E}_i^{*(b)}}{E_{\max}}, \qquad I_i^{*(b)} = \frac{\bar{S}_i^{*(b)}}{S_{\max}}, \tag{A.12}$$

and

$$R_i^{*(b)} = L_i^{*(b)} I_i^{*(b)}. \tag{A.13}$$

The percentile-based 95% bootstrap confidence interval was then

$$\mathrm{CI}_{0.95}(R_i) = \left[Q_{0.025}\left(R_i^{*(1)}, \ldots, R_i^{*(B)} \right), Q_{0.975}\left(R_i^{*(1)}, \ldots, R_i^{*(B)} \right) \right]. \tag{A.14}$$

The resulting intervals therefore quantify sampling uncertainty in the protocol-level composite index under repeated record-level resampling. They should not be interpreted as prediction intervals for future deployments.

A.4. Kruskal–Wallis omnibus test

For each outcome $X \in \{E, S\}$, all $N = 4378$ observations were pooled and ranked from 1 to N. Tied observations were assigned their average rank, which is important because CVSS subscores contain many repeated values.

Let r_{ij} be the pooled rank of observation X_{ij} and let

$$T_i = \sum_{j=1}^{n_i} r_{ij} \tag{A.15}$$

be the rank sum for protocol i. The uncorrected Kruskal–Wallis statistic was

$$H_{\mathrm{raw}} = \frac{12}{N(N+1)} \sum_{i=1}^{k} \frac{T_i^2}{n_i} - 3(N+1). \tag{A.16}$$

Let t_ℓ denote the number of observations in tied-value group ℓ, where $\ell = 1, \ldots, g$. The tie-correction factor was

$$C = 1 - \frac{\sum_{\ell=1}^{g} \left(t_\ell^3 - t_\ell \right)}{N^3 - N}. \tag{A.17}$$

The tie-corrected test statistic was therefore

$$H = \frac{H_{\text{raw}}}{C}. \tag{A.18}$$

Under the null hypothesis and the usual large-sample approximation,

$$H \sim \chi^2_{k-1}. \tag{A.19}$$

The omnibus p-value was calculated as

$$p = 1 - F_{\chi^2_{k-1}}(H), \tag{A.20}$$

where $F_{\chi^2_{k-1}}$ is the cumulative distribution function of a chi-squared distribution with $k - 1 = 4$ degrees of freedom.
For each outcome, the hypotheses were

$$H_0 : F_1(x) = F_2(x) = \cdots = F_k(x), \tag{A.21}$$

against

$$H_1 : \text{at least one protocol distribution differs.} \tag{A.22}$$

The Kruskal–Wallis test is therefore an omnibus comparison of the protocol-level distributions. It should not be described exclusively as a test of means or medians unless additional distributional assumptions are made.

A.5. Ordinal eta-squared effect size

The omnibus effect size was calculated as ordinal eta-squared based on the tie-corrected Kruskal–Wallis statistic:

$$\eta^2_H = \frac{H - k + 1}{N - k}. \tag{A.23}$$

For Exploitability,

$$\eta^2_{H,E} = \frac{9.210 - 5 + 1}{4378 - 5} = \frac{5.210}{4373} = 0.001191 \approx 0.0012. \tag{A.24}$$

Thus, the protocol-related Exploitability effect was negligible.
For Impact,

$$\eta^2_{H,S} = \frac{255.983 - 5 + 1}{4378 - 5} = \frac{251.983}{4373} = 0.057622 \approx 0.058. \tag{A.25}$$

Thus, the protocol-related Impact effect was measurable but modest. Because η^2_H is derived from ranked data, it is used as a comparative effect-size indicator and should not be interpreted as an exact proportion of variance in the original CVSS subscores.

A.6. Dunn post-hoc comparisons

Pairwise Dunn comparisons were conducted only when the corresponding Kruskal–Wallis omnibus test was statistically significant. Let

$$\bar{r}_i = \frac{T_i}{n_i} \tag{A.26}$$

denote the mean pooled rank of protocol i. The tie-adjusted rank-variance term was

$$V_r = \frac{N(N+1)}{12} - \frac{\sum_{\ell=1}^{g} \left(t_\ell^3 - t_\ell\right)}{12(N-1)}. \tag{A.27}$$

For protocols i and j, Dunn's standardized statistic was

$$z_{ij} = \frac{\bar{r}_i - \bar{r}_j}{\sqrt{V_r\left(\frac{1}{n_i} + \frac{1}{n_j}\right)}}. \tag{A.28}$$

The unadjusted two-sided pairwise p-value was

$$p_{ij} = 2\left[1 - \Phi\left(\left|z_{ij}\right|\right)\right], \tag{A.29}$$

where $\Phi(\cdot)$ is the standard normal cumulative distribution function.
With $k = 5$ protocol families, the number of possible pairwise comparisons was

$$m = \binom{k}{2} = \frac{k(k-1)}{2} = 10. \tag{A.30}$$

A.7. Holm correction for multiple comparisons

The $m = 10$ unadjusted Dunn p-values were ordered as

$$p_{(1)} \le p_{(2)} \le \cdots \le p_{(m)}. \tag{A.31}$$

For the rth ordered comparison, Holm's adjusted p-value was calculated as

$$p_{(r)}^{\text{Holm}} = \min\left\{1, \max_{1\le \ell \le r}\left[(m-\ell+1)p_{(\ell)}\right]\right\}. \tag{A.32}$$

Equivalently, Holm's sequential decision rule compares each ordered p-value with

$$\frac{\alpha}{m-r+1}, \tag{A.33}$$

starting from the smallest p-value and stopping when the first non-rejection is encountered. This procedure controls the family-wise error rate across the ten pairwise comparisons.

A.8. Decision sequence and reported results

The complete inferential decision sequence was as follows:

1. Apply the tie-corrected Kruskal–Wallis test separately to the individual Exploitability and Impact observations.
2. Calculate η_H^2 for each omnibus test, irrespective of statistical significance, to quantify the magnitude of the observed protocol-related difference.
3. Conduct Dunn pairwise comparisons only when the corresponding omnibus test is statistically significant at $\alpha = 0.05$.
4. Apply Holm correction to all ten Dunn comparisons belonging to the significant outcome.

For Exploitability, the result was

$$H(4) = 9.210, \qquad p = .0561, \qquad \eta_H^2 \approx 0.0012. \tag{A.34}$$

Because the omnibus Exploitability test was not statistically significant, no Exploitability pairwise differences were interpreted.
For Impact, the result was

$$H(4) = 255.983, \qquad p < .001, \qquad \eta_H^2 \approx 0.058. \tag{A.35}$$

The significant Impact omnibus result warranted Dunn's post-hoc analysis. After Holm correction, Wi-Fi exhibited significantly higher Impact scores than Bluetooth,

$$p_{\text{Holm}} < 0.001, \tag{A.36}$$

and proprietary RF,

$$p_{\text{Holm}} = 0.0156. \tag{A.37}$$

The remaining pairwise Impact comparisons did not remain statistically significant after Holm correction.
All statistical calculations were performed using the unrounded CVSS observations and unrounded intermediate results. Rounding was applied only when presenting the final values in the tables and manuscript text.

Appendix B. Derivation of the CVSS v3.x Normalization Constants

The normalization constants were derived from the official CVSS v3.x Base-metric equations and permitted metric weights rather than from the study dataset [34]. The Exploitability subscore is

$$E = 8.22 \times AV \times AC \times PR \times UI. \tag{B.1}$$

Using the maximum permitted weights, $AV : N = 0.85$, $AC : L = 0.77$, $PR : N = 0.85$, and $UI : N = 0.85$, gives

$$\begin{aligned} E_{\max} &= 8.22(0.85)(0.77)(0.85)(0.85) \\ &= 3.887042775 \approx 3.887. \end{aligned} \tag{B.2}$$

For the Impact subscore, the maximum Confidentiality, Integrity, and Availability weights are obtained when all three impacts are High, such that $C = I = A = 0.56$. Therefore,

$$\begin{aligned} ISS_{\max} &= 1 - (1-C)(1-I)(1-A) \\ &= 1 - (1-0.56)^3 \\ &= 0.914816. \end{aligned} \tag{B.3}$$

For Changed Scope, which produces the largest attainable Impact subscore over the permitted CVSS Base-metric combinations,

$$S_{\max} = 7.52(ISS_{\max} - 0.029) - 3.25(ISS_{\max} - 0.02)^{15} = 6.0477304915 \approx 6.048. \tag{B.4}$$

Thus, $E_{\max} = 3.887$ and $S_{\max} = 6.048$ are formula-derived normalization constants and not observed sample maxima. The latter is the maximum attainable CVSS v3.x Impact subscore and should not be confused with the maximum CVSS Base Score of 10.0.

References

[1] A. Gobinath, P. Rajeswari, N. Suresh Kumar, M. Anandan, Internet of Medical Things (IoMT), John Wiley & Sons, Ltd, 2024, pp. 91–105. https://doi.org/10.1002/9781394275472.ch5

[2] P. Matthew, S. Mchale, X. Deng, G. Nakhla, M. Trovati, N. Nnamoko, E. Pereira, H. Zhang, M. Raza, A review of the state of the art for the internet of medical things, Sci 7 (2) (2025). https://www.mdpi.com/2413-4155/7/2/36. https://doi.org/10.3390/sci7020036

[3] K. Katzis, R. Jones, G. Despotou, The challenges of balancing safety and security in implantable medical devices, Stud. Health Technol. Inform. 226 (2016) 25–28. https://doi.org/10.3233/978-1-61499-664-4-25

[4] H. Verma, N. Chauhan, L.K. Awasthi, A comprehensive review of 'Internet of healthcare things': networking aspects, technologies, services, applications, challenges, and security concerns, Comput. Sci. Rev. 50 (2023) 100591. https://www.sciencedirect.com/science/article/pii/S1574013723000588. https://doi.org/10.1016/j.cosrev.2023.100591

[5] S.A. Baho, J. Abawajy, Analysis of consumer IoT device vulnerability quantification frameworks, Electronics 12 (5) (2023). https://www.mdpi.com/2079-9292/12/5/1176. https://doi.org/10.3390/electronics12051176

[6] A.O. Affia, H. Finch, W. Jung, I.A. Samori, L. Potter, X.-L. Palmer, IoT health devices: exploring security risks in the connected landscape, IoT 4 (2) (2023) 150–182. https://www.mdpi.com/2624-831X/4/2/9. https://doi.org/10.3390/iot4020009

[7] S. Bayyapu, Impact of the internet of medical things (IoMT) on healthcare cybersecurity, Int. J. Innov. Eng. Manag. Res. 12 (2023) 146–153.

[8] W.H. Kruskal, W.A. Wallis, Use of ranks in one-criterion variance analysis, J. Am. Stat. Assoc. 47 (260) (1952) 583–621. https://doi.org/10.1080/01621459.1952.10483441

[9] M. Tomczak, E. Tomczak, The need to report effect size estimates revisited: an overview of some recommended measures of effect size, Trends Sport Sci. 21 (1) (2014) 19–25. https://tss.awf.poznan.pl/pdf-188960-110189?filename=The-need-to-report-effect.pdf.

[10] F. Fiel Peres, Effect sizes for nonparametric tests, Biochem. Med. 36 (1) (2026) 010101. https://doi.org/10.11613/BM.2026.010101

[11] O.J. Dunn, Multiple comparisons using rank sums, Technometrics 6 (3) (1964) 241–252. https://doi.org/10.1080/00401706.1964.10490181

[12] S. Holm, A simple sequentially rejective multiple test procedure, Scand. J. Stat. 6 (2) (1979) 65–70. https://www.jstor.org/stable/4615733.

[13] T.A. Shaikh, T. Rasool, P. Verma, Machine intelligence and medical cyber-physical system architectures for smart healthcare: taxonomy, challenges, opportunities, and possible solutions, Artif. Intell. Med. 146 (2023) 102692. https://www.sciencedirect.com/science/article/pii/S0933365723002063. https://doi.org/10.1016/j.artmed.2023.102692

[14] A. Barua, M.A. Al Alamin, M.S. Hossain, E. Hossain, Security and privacy threats for bluetooth low energy in IoT and wearable devices: a comprehensive survey, IEEE Open J. Commun. Soc. 3 (2022) 251–281. https://doi.org/10.1109/OJCOMS.2022.3149732

[15] J. Bellardo, S. Savage, 802.11 Denial-of-Service attacks: real vulnerabilities and practical solutions, in: Proceedings of the 12th USENIX Security Symposium, USENIX, 2003, pp. 15–28.

[16] T. Zillner, S. Strobl, ZigBee Exploited: The Good, the Bad and the Ugly, Black Hat USA (2015). https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf.

[17] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, A. Chehab, LoRaWAN security survey: issues, threats and possible mitigation techniques, Internet Things 12 (2020) 100303. https://www.sciencedirect.com/science/article/pii/S2542660520301359. https://doi.org/10.1016/j.iot.2020.100303

[18] F. Alsubaei, A. Abuhussein, S. Shiva, Security and privacy in the internet of medical things: taxonomy and risk assessment, Future Gener. Comput. Syst. 123 (2022) 58–71. https://doi.org/10.1016/j.future.2021.04.031

[19] J. Tournier, F. Lesueur, F.L. Mouël, L. Guyon, H. Ben-Hassine, A survey of IoT protocols and their security issues through the lens of a generic IoT stack, Internet Things 16 (2021) 100264. https://www.sciencedirect.com/science/article/pii/S2542660520300986. https://doi.org/10.1016/j.iot.2020.100264

[20] K. Svandova, Z. Smutny, Internet of medical things security frameworks for risk assessment and management: a scoping review, J. Multidiscip. Healthc. 17 (2024) 2281–2301. https://doi.org/10.2147/JMDH.S459987

[21] L. Dzamesi, N. Elsayed, A review on the security vulnerabilities of the IoMT against malware attacks and DDoS, arXiv preprint arXiv:2501.07703 (2025).

[22] M. Asif, M. Abrar, A. Salam, F. Amin, F. Ullah, S. Shah, H. AlSalman, Intelligent two-phase dual authentication framework for internet of medical things, Sci. Rep. 15 (2025) 1760. https://doi.org/10.1038/s41598-024-84713-5

[23] S.S. Ahamad, M. Al-Shehri, I. Keshta, A secure and resilient scheme for telecare medical information systems with threat modeling and formal verification, IEEE Access 10 (2022) 120227–120244. https://doi.org/10.1109/ACCESS.2022.3217230

[24] A. Shostack, Experiences threat modeling at microsoft, IEEE Secur. Priv. 3 (1) (2005) 61–63. https://doi.org/10.1109/MSP.2005.22

[25] M. Ryan, Bluetooth: with low energy comes low security, in: Proceedings of the 7th USENIX Conference on Offensive Technologies, WOOT'13, USENIX Association, USA, 2013, p. 4.

[26] M. Cäsar, T. Pawelke, J. Steffan, G. Terhorst, A survey on bluetooth low energy security and privacy, Comput. Netw. 205 (2022) 108712. https://www.sciencedirect.com/science/article/pii/S1389128621005697. https://doi.org/10.1016/j.comnet.2021.108712

[27] LoRa Alliance, LoRaWAN Security Whitepaper, Technical Report, LoRa Alliance, 2020. Accessed: 2025-06-20, https://lora-alliance.org/wp-content/uploads/2020/11/lorawan_security_whitepaper.pdf.

[28] M. Ngamboé, P. Berthier, N. Ammari, K. Dyrda, J.M. Fernandez, Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED), Int. J. Inf. Secur. 20 (4) (2021) 621–645. https://doi.org/10.1007/s10207-020-00522-7

[29] D.C. Klonoff, J. Han, The first recall of a diabetes device because of cybersecurity risks, J. Diabetes Sci. Technol. 13 (5) (2019) 817–820. https://journals.sagepub.com/doi/10.1177/1932296819865655. https://doi.org/10.1177/1932296819865655

[30] E. Anthi, L. Williams, V. Ieropoulos, T. Spyridopoulos, Investigating radio frequency vulnerabilities in the internet of things (IoT), IoT 5 (2) (2024) 356–380. https://doi.org/10.3390/iot5020018

[31] T. Simões, T. Cruz, B. Sousa, P. Simões, A security-conscious primer on LoRa and LoRaWAN technologies, Eur. Conf. Cyber Warf. Secur. 24 (2025) 638–646. https://doi.org/10.34190/eccws.24.1.3575

[32] S. Chaudhary, R. Kakkar, N.K. Jadav, A. Nair, R. Gupta, S. Tanwar, S. Agrawal, M.D. Alshehri, R. Sharma, G. Sharma, I.E. Davidson, A taxonomy on smart healthcare technologies: security framework, case study, and future directions, J. Sens. 2022 (1) (2022) 1863838. https://doi.org/10.1155/2022/1863838

[33] Joint Task Force Transformation Initiative, Guide for Conducting Risk Assessments, Technical Report Special Publication 800-30 Revision 1, National Institute of Standards and Technology (NIST), 2012. https://doi.org/10.6028/NIST.SP.800-30r1

[34] S.T. Response, Forum of Incident and (FIRST), Common Vulnerability Scoring System v3.1: Specification Document, 2026, (https://www.first.org/cvss/v3.1/specification-document). Accessed: 21 August 2026.

[35] A. Hoeller, R. Toegl, Trusted platform modules in cyber-physical systems: on the interference between security and dependability, in: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2018, pp. 136–144. https://doi.org/10.1109/EuroSPW.2018.00026

[36] D. Sethia, D. Gupta, H. Saran, NFC secure element-based mutual authentication and attestation for IoT access, IEEE Trans. Consum. Electron. 64 (4) (2018) 470–479. https://doi.org/10.1109/TCE.2018.2873181

[37] B. Romansky, T. Mazzuchi, S. Sarkani, Extending the update framework (TUF) for industrial control system applications, in: SoutheastCon 2024, 2024, pp. 1571–1576. https://doi.org/10.1109/SoutheastCon52093.2024.10500028
[38] Wi-Fi Alliance, WPA3 Specification Version 3.4, 2024, (Technical specification). Online; accessed Jul. 12, 2025, https://www.wi-fi.org/system/files/WPA3%20Specification%20v3.4.pdf.
[39] S. Rattal, A. Badri, M. Moughit, E. Miloud Ar-Reyouchi, K. Ghoumid, AI-driven optimization of low-energy IoT protocols for scalable and efficient smart healthcare systems, IEEE Access 13 (2025) 48401–48415. https://doi.org/10.1109/ACCESS.2025.3551224