Scientific Research Publishing

Journal of Information Security, 2026, 17(4), 406-430
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Healthcare Internet of Things (HIoT) Threat Modelling Using STRIDE-LM

Abdulburhan Mohamed, Brian Maodza

Faculty of Science and Technology, Emeris, The Independent Institute of Education, Johannesburg, South Africa
Email: bmaodza02@gmail.com

How to cite this paper: Mohamed, A. and Maodza, B. (2026) Healthcare Internet of Things (HIoT) Threat Modelling Using STRIDE-LM. *Journal of Information Security*, **17**, 406-430.
https://doi.org/10.4236/jis.2026.174019

Received: July 13, 2026
Accepted: August 22, 2026
Published: August 25, 2026

Abstract

The integration of the Healthcare Internet of Things (HIoT) in health delivery systems has transformed patient care through real-time monitoring and data-driven decision-making, yet it introduces significant cybersecurity vulnerabilities that threaten patient safety and data privacy. The research addresses the critical gap in understanding and modelling cybersecurity threats specific to healthcare environments by applying the STRIDE-LM (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege and Lateral Movement) threat modelling technique to HIoT architectures. Through a Systematic Literature Review (SLR), the research reviewed 35 peer-reviewed publications to examine HIoT's four-layer architecture (Physical, Network, Processing and Application layers) and categorises cybersecurity threats across the seven STRIDE-LM classifications. The Design Science Research (DSR) methodology was used to model the threats using STRIDE-LM. Distinct threat patterns were identified across the architectural layers, revealing that many medical devices operate with outdated firmware and that critical implementation gaps persist despite widespread threat awareness. The findings demonstrate that STRIDE-LM, when adapted for healthcare contexts to incorporate patient safety considerations, provides literature-based coverage for threat identification and modelling *i.e.* coverage established against the reviewed literature rather than demonstrated operational effectiveness, enabling healthcare stakeholders to prioritise security investments and develop mitigation strategies that address the unique complexities of healthcare environments.

Keywords

Medical Device Security, Patient Safety, Connected Medical Devices, Clinical Data Privacy, Lateral Movement, Cybersecurity Vulnerabilities

1. Introduction

The rapid integration of digital healthcare technologies has fundamentally transformed medical service delivery, with the Healthcare Internet of Things (HIoT) emerging to integrate interconnected medical devices, sensors and systems that enhance patient care through real-time monitoring and data collection [1]. HIoT facilitates data exchange between wearable devices, implantable sensors and centralized healthcare systems, enabling healthcare providers to deliver more proactive treatment [2]. However, as healthcare facilities increasingly adopt these IoT technologies to improve operational efficiency and patient outcomes, significant security vulnerabilities have emerged that threaten patient safety, data privacy and healthcare services [3].

This research addressed a critical gap in cybersecurity threat understanding within healthcare IoT environments by applying the STRIDE-LM (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege and Lateral Movement) threat modelling technique, a systematically reviewed and repeatable approach for security threat identification [4]. The research examined HIoT architecture through a Systematic Literature Review (SLR) to develop a structured understanding of cybersecurity vulnerabilities that can be compromised and negatively affect the security of healthcare systems.

1.1. Background

HIoT allows medical devices to collect, process and transmit sensitive patient data, creating significant opportunities for improved healthcare delivery while introducing complex security challenges [5]. HIoT includes wearable health monitors, implantable medical devices, remote patient monitoring systems and smart hospital infrastructure that enable continuous patient monitoring and real-time data transmission. The interconnected architecture of HIoT presents cybersecurity challenges that extend beyond traditional data breaches, with potential consequences including compromised patient data privacy, disruption of essential healthcare operations and life-threatening risks for patients relying on these technologies [6]. Unlike traditional IT devices and systems, HIoT devices operate with limited resources and inconsistent security protocols, with healthcare environments introducing additional complexity through life-critical applications [7].

Current security approaches fail to address the unique complexities of healthcare environments, with traditional security measures proving inadequate for evolving cyber threats within healthcare settings [8]. While existing research addresses broad IoT security vulnerabilities [9], a critical gap remains in threat modelling specific to healthcare environments [10]. The STRIDE-LM threat modelling technique, which extends Microsoft's STRIDE technique by incorporating lateral movement capabilities, presents a structured approach for addressing this gap [11]. Although STRIDE-LM has demonstrated effectiveness in other IoT domains like smart agriculture [12], its application to healthcare IoT environments remains largely unexplored, representing a significant opportunity to develop comprehen-

sive threat understanding specific to healthcare contexts [6].

1.2. Problem Statement

The integration of HIoT devices in healthcare has transformed patient care through remote monitoring, real-time health tracking and data-driven decision-making [13]. However, the interconnected architecture of HIoT introduces significant cybersecurity vulnerabilities that can compromise patient data privacy and the availability of critical healthcare services [6]. Cyber-attacks on HIoT can lead to the exposure of sensitive medical information and disruption of essential healthcare operations, with potentially life-threatening consequences for patients [14]. Despite the growing adoption of HIoT, current security measures and threat modelling techniques remain inadequate in addressing the evolving cyber threats targeting HIoT, as traditional security approaches often fail to account for the unique complexities of healthcare environments [14].

1.3. Purpose, Research Questions and Objectives

The purpose of this research was to model HIoT threats using STRIDE-LM. Additionally, the research aimed to provide healthcare stakeholders with an understanding of how HIoT operates by identifying the architectural components used in HIoT. The research was guided by the following three research questions:

1) What are the different architectural components used in HIoT?

2) What are the cybersecurity threats in HIoT?

3) How can the STRIDE-LM threat modelling technique be used to model threats in HIoT?

The remainder of this article is structured as follows. Section 2 presents the theoretical foundation of the research. Section 3 reviews the literature on HIoT architecture, STRIDE-LM threat modelling and cybersecurity threats in HIoT. Section 4 describes research design and methodology. Section 5 presents the findings and their interpretation, Section 6 discusses how the research questions were addressed, and Section 7 concludes the article.

2. Theoretical Foundation

The Protection Motivation Theory (PMT), originated by Rogers (1975), examines how individuals respond to threats through threat appraisal (evaluating severity and vulnerability) and coping appraisal (assessing the ability and effectiveness of protective measures). PMT is particularly valuable for security in HIoT as it helps explain why healthcare stakeholders might recognize security risks but fail to allocate sufficient resources to cybersecurity [15]. When applied to STRIDE-LM threat modelling, PMT provides an approach for prioritizing threats based on perceived impact and explains why certain threats, such as lateral movement vulnerabilities, often receive insufficient attention despite their severity [16].

The Technology Threat Avoidance Theory (TTAT), developed by [17], addresses the psychological factors influencing how users perceive and respond to

technological threats. TTAT is highly relevant to security within HIoT as it helps explain why healthcare professionals might compromise security protocols despite awareness of threats, such as disabling security features on HIoT devices to increase operational efficiency, thereby creating vulnerabilities exploitable through tampering or elevation of privilege attacks. When applied to STRIDE-LM threat modelling, TTAT provides insights into how organisational factors influence the effectiveness of security measures.

The Theory of Planned Behavior (TPB), proposed by [18], explores how behaviors are shaped by attitudes, subjective norms and perceived behavioral control. TPB is essential for security in HIoT as it highlights the gap between security intentions and implementation. The theory's emphasis on subjective norms is particularly relevant in healthcare contexts, where professional culture and organisational priorities significantly impact security measures.

Together, these three theories provide a theoretical foundation for addressing the complex cybersecurity challenges unique to HIoT: PMT focuses on threat perception and protective motivation, TTAT emphasizes threat avoidance behaviors and TPB examines factors influencing security implementation. By integrating these theories with STRIDE-LM threat modelling, the research provides insights into security challenges in HIoT, considering both technical vulnerabilities and the human and organisational factors that significantly impact security effectiveness in healthcare environments.

It should be emphasised that PMT, TTAT and the TPB are employed in this study as interpretive lenses rather than as operational coding frameworks. Their constructs did not inform the coding scheme or the construction of the threat model, both of which were structured deductively by the seven STRIDE-LM categories and the four architectural layers. Instead, the theories are drawn upon in Section 5 to interpret and explain patterns that emerged from that analysis, in particular the persistent gap between threat awareness and mitigation. No claim is made that the constructs of these theories were operationalised, measured or empirically tested in this research.

3. Literature Review

HIoT has emerged because of the rapid digitalization of healthcare, enabled by the increasing integration of IoT technologies within medical environments. As healthcare systems become increasingly interconnected, the utilisation of HIoT devices, which collect, process and transmit sensitive patient data, creates significant opportunities for improving healthcare delivery while also introducing complex security challenges [19]. The security risks associated with HIoT require significant attention due to the sensitive nature of patient data and the effects on patient safety and well-being [20]. This review examines the relationship between HIoT architectures and cybersecurity vulnerabilities, structured around the three research questions: It first analyses the layered HIoT architecture, then evaluates the STRIDE-LM threat modelling technique and its applications in other IoT do-

mains and finally analyses cybersecurity threats specific to HIoT, emphasising vulnerabilities that directly impact patient care and data integrity.

3.1. HIoT Architecture

HIoT architecture represents a complex network of interconnected components designed to improve patient care through data collection and analysis. The literature reveals a four-layer architectural model forming the foundation of HIoT systems, with each layer presenting distinct security challenges.

Physical Layer. At the physical layer, HIoT encompasses various medical devices that collect, process and transmit patient data. Reference [10] categorises these devices into three primary types which are implantable devices such as pacemakers and insulin pumps, wearable sensors monitoring vital signs, and stationary medical equipment such as infusion pumps and ventilators. Reference [10] emphasised that this layer is particularly vulnerable to physical tampering, where attackers can manipulate devices to compromise functionality or extract sensitive information. This vulnerability is intensified by the fact that many medical devices operate with outdated firmware that cannot be readily updated without disrupting critical healthcare services; [19] estimated that as many as 72% of medical devices run outdated firmware. This figure is reported by [19] in a survey-style review of networked medical devices that aggregates vendor advisories and secondary vulnerability datasets rather than auditing a defined device population; it should therefore be read as indicative of a broad installed base rather than a measured prevalence in a single clinical setting, creating potential for substantial attack and device exploitation.

Network Layer. The network layer facilitates data transmission between physical devices and processing systems through various communication protocols. Reference [21] identified several common protocols in HIoT environments, which include Bluetooth, Wi-Fi, ZigBee and cellular technologies such as 5G. Reference [22] argued that these technologies significantly complicate security implementation, as each protocol introduces unique vulnerabilities requiring separate security measures; their research reveals that approximately 65% of hospital Wi-Fi networks lack proper separation reported by [22] on the basis of a security risk assessment of reviewed hospital network deployments rather than a randomised sample of hospitals, allowing attackers to access critical patient databases. While [23] suggested that the diversity of protocols can enhance security through defence in depth, [24] countered this perspective by highlighting that healthcare's resource constraints often make such comprehensive security approaches impractical. Reference [20] further noted that the wireless nature of communication within HIoT introduces additional vulnerabilities related to signal interception.

Processing Layer. The processing layer serves as middleware between network communications and applications, handling data aggregation, filtering and analysis of collected health information [19]. According to [25], this layer is vulnerable to unauthorised data manipulation during processing, where attackers can poten-

tially manipulate health data before it reaches healthcare stakeholders. Reference [26] identified that approximately 35% of healthcare stakeholders lack robust authentication methods a characterisation drawn by [26] from secondary security-engineering literature on healthcare processing environments rather than from a measured facility census, creating opportunities for dangerous modifications to patient data that might evade detection.

Application Layer. The application layer covers software systems that analyse and visualise processed data collected from HIoT devices, including electronic health record (EHR) systems and remote monitoring platforms [19]. Reference [25] highlighted that vulnerabilities at this layer often stem from poor software development practices, including inadequate input validation, insufficient access controls and improper session management. Reference [26] revealed that approximately 40% of healthcare applications employ weak authentication methods likewise reported by [26] as an indicative estimate synthesised from the secondary literature rather than derived from a primary audit of a defined application sample, creating significant opportunities for unauthorised access.

The integration between these four architectural layers introduces additional vulnerabilities that extend beyond the individual components. Reference [27] emphasised that security weaknesses often emerge between layers, where different security assumptions and implementations create inconsistencies that attackers can exploit, suggesting the need for a comprehensive rather than layer-by-layer approach to security in HIoT. Reference [22] reinforced the importance of understanding this layered architectural structure for applying STRIDE-LM to model threats in HIoT effectively, while [28] emphasised the importance of end-to-end encryption across all architectural components, acknowledging that achieving such consistency remains challenging in healthcare environments due to technical and organisational constraints.

3.2. STRIDE-LM Threat Modelling in HIoT

The original STRIDE technique, as described by [11], categorises security threats into six types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege. While this technique has proven valuable for identifying potential vulnerabilities in various domains, [29] noted that it was initially developed for traditional computing environments and requires adaptation for specific domains such as healthcare.

The extension to STRIDE-LM, incorporating Lateral Movement as a seventh threat category, represents a significant advancement of the technique. According to [12], lateral movement threats involve attackers leveraging initial access to move between different systems within a network, potentially escalating their capabilities and access rights. This addition is particularly relevant for HIoT, where interconnected devices create multiple potential entry points for attackers. Reference [12] demonstrated STRIDE-LM's application in agricultural IoT environments, highlighting its effectiveness in identifying threats that might be over-

looked using traditional security assessment approaches. However, [30] argued that threat modelling techniques like STRIDE-LM may not adequately address healthcare-specific security requirements without significant adaptation, suggesting that threat modelling in healthcare should incorporate additional considerations related to patient safety.

Using STRIDE-LM in healthcare environments presents several challenges that must be addressed for effective implementation. Reference [31] identified three key adaptation challenges: integrating patient safety considerations into threat assessment, accounting for the unique environment of healthcare, and addressing the diverse technical capabilities of healthcare stakeholders. Reference [6] further highlighted the dynamic nature of healthcare environments, where changes in device configurations and system integrations can significantly impact security. Reference [22] added that patient safety impact should be considered for each identified threat, acknowledging that the consequences of security breaches in healthcare extend beyond data loss and could lead to physical harm. However, [27] cautioned that complex threat modelling techniques may see reduced adoption in healthcare environments where security resources are often limited.

3.3. Cybersecurity Threats and Challenges in HIoT

HIoT environments face numerous cybersecurity threats that exploit vulnerabilities across the architectural layers. These threats are distinguished by their potential to impact not only data confidentiality but also patient safety and healthcare delivery.

Patient data privacy represents a primary security concern in HIoT. Reference [19] identified several common attacks targeting patient data privacy, including unauthorised access to medical records, interception of unencrypted data transmissions and exploitation of authentication weaknesses. These attacks primarily align with the Information Disclosure category in STRIDE-LM but may involve other threat types, such as Spoofing, when attackers impersonate authorised users. Reference [14] emphasised that data privacy breaches in healthcare carry more severe consequences than in many other domains, as they may reveal highly sensitive information about patients' health conditions, treatments and personal details.

Threats to healthcare operations represent a particularly concerning category, as they may directly impact patient care. Reference [6] identified attacks including manipulation of medical device readings and alteration of medication dosage instructions, aligning primarily with the Tampering category but potentially involving Elevation of Privilege when attackers gain administrative access to clinical systems. Reference [20] described scenarios where compromised medical devices could deliver incorrect treatments, potentially causing direct physical harm to patients, while [32] highlighted the risks of manipulated data leading to incorrect diagnoses and treatment decisions.

Service availability represents another critical security concern in healthcare environments. Reference [33] identified common availability attacks including

Distributed Denial of Service (DDoS) attacks targeting critical infrastructure, ransomware attacks encrypting essential clinical data and device jamming affecting wireless medical equipment, aligning primarily with the Denial-of-Service category. Reference [15] described scenarios where the unavailability of critical systems could delay urgent care delivery, while [2] broadened this perspective by highlighting unintentional availability threats, arguing that system issues, resource constraints and configuration errors often cause more frequent availability challenges than deliberate attacks.

Finally, the interconnected nature of HIoT creates unique vulnerabilities related to lateral movement between systems. Reference [13] identified common lateral movement techniques in healthcare environments, including exploitation of shared credentials and leveraging unpatched vulnerabilities in network infrastructure, while [10] broaden this perspective by highlighting organisational factors that contribute to these vulnerabilities.

In synthesis, the literature reveals that security vulnerabilities in HIoT extend beyond traditional cybersecurity concerns: breaches can lead to patient harm through manipulated medical device readings, altered medication dosages or disrupted healthcare services [20]. While STRIDE-LM allows for structured threat modelling, it requires significant adaptation to effectively address healthcare-specific concerns, and there remains insufficient research on adapting threat modelling techniques specifically for healthcare environments [26]. This gap motivated the present research.

4. Research Design and Methodology

This research followed a qualitative design combining two complementary methodological components. First, a Systematic Literature Review (SLR) was conducted and reported in accordance with the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines [33] to identify the architectural components of HIoT and the cybersecurity threats affecting healthcare environments. Second, the Design Science Research (DSR) methodology was used to model the identified threats, treating the STRIDE-LM identified threats for HIoT as the designed artifact. An SLR approach was appropriate as it allowed for an in-depth exploration of HIoT architecture, threat modelling using STRIDE-LM and security vulnerabilities without requiring statistical data analysis, while the combination of the two methodologies ensured that the artifact was rigorously grounded in the existing knowledge base. According to [34], DSR requires thorough and rigorous grounding in existing theories, which was achieved here through the PRISMA-guided systematic review.

4.1. Systematic Literature Review Following PRISMA 2020

Eligibility criteria. The review targeted peer-reviewed academic literature, technical documentation and industry reports published between 2015 and 2025 addressing HIoT architecture, cybersecurity threats and threat modelling tech-

niques, with individual publication as the unit of analysis. Consistent with PRISMA 2020, explicit inclusion and exclusion criteria were defined a priori and applied uniformly throughout the selection process, as presented in Table 1.

Table 1. Inclusion and exclusion criteria for study selection.

Inclusion criteria	Exclusion criteria
Published in a peer-reviewed academic journal or conference between 2015 and 2025	Focused exclusively on non-healthcare IoT domains without relevant insights for HIoT
Directly addresses HIoT architecture, cybersecurity threats in healthcare, or threat modelling techniques (with particular emphasis on STRIDE-LM)	Provides only high-level discussion or overviews without sufficient technical depth
Provides technical or theoretical detail sufficient for data extraction	Duplicates findings already captured from other included sources
Accessible in English (full text available)	Lacks credible peer review or academic rigour

Information sources and search strategy. Search was conducted across seven academic databases: IEEE Xplore, ScienceDirect, Springer, EBSCO, PubMed, ResearchGate and Google Scholar. The search strategy combined predefined keywords, including "Healthcare Internet of Things", "HIoT", "cybersecurity", "security threats", "vulnerabilities", "STRIDE", "STRIDE-LM", "threat modelling" and "healthcare security", applied consistently across databases.

Table 2. Reproducible search strategy and records retrieved by source.

Database	Search string (as adapted to database syntax)	Fields searched	Records retrieved
IEEE Xplore	("Healthcare Internet of Things" OR "HIoT" OR "IoMT") AND ("cybersecurity" OR "security threat*" OR "vulnerabilit*") AND ("STRIDE*" OR "threat model*")	Title, Abstract, Author Keywords	312
ScienceDirect	Core expression with connectors adapted (limited wildcard expansion permitted by the interface)	Title, Abstract, Keywords	287
Springer Link	Core expression with "HIoT"/"IoMT" synonyms; exact phrases in quotation marks	Title, Abstract, Keywords	254
EBSCO (Academic Search/CINAHL)	Core expression with proximity operators (N/near) applied to key phrases	Title, Abstract, Subject terms	198
PubMed	("Internet of Things"[MeSH] OR HIoT OR IoMT) AND (cybersecurity OR security[tiab]) AND ("threat model*"[tiab])	Title/Abstract [tiab], MeSH	176
ResearchGate	Core keyword expression (no reliable field restriction available)	Full text	143
Google Scholar	"Healthcare Internet of Things" "threat modelling" STRIDE (allintitle used where supported)	Full text	310
Total	—	—	1680

To ensure reproducibility, the search strategy is reported in full. Searches were executed between 15 January 2025 and 28 February 2025, with a final verification search on 10 March 2025 to capture newly indexed records. In databases support-

ing fielded search (IEEE Xplore, ScienceDirect, Springer Link, EBSCO and PubMed), queries were restricted to the Title, Abstract and Author Keywords fields; ResearchGate and Google Scholar, which do not support reliable field restriction, were searched on full text and screened by title and abstract. The core Boolean expression was: ("Healthcare Internet of Things" OR "HIoT" OR "Internet of Medical Things" OR "IoMT") AND ("cybersecurity" OR "security threat*" OR "vulnerabilit*") AND ("STRIDE" OR "STRIDE-LM" OR "threat model*"). Table 2 shows the database-specific search strings, the fields searched and the number of records retrieved from each source; the totals reconcile with the 1680 records entering the PRISMA identification phase.

Selection process. Study selection followed the PRISMA 2020 flow of identification, screening, eligibility assessment and inclusion as illustrated in the PRISMA flow diagram in Figure 1 [33]. In the identification phase, 1680 records were retrieved from the seven databases and consolidated using reference-mapping software (Connected Papers and Litmaps), through which 423 duplicate records were removed. In the screening phase, the titles and abstracts of the remaining 1257 records were assessed against the eligibility criteria in Table 1, and 1108 clearly irrelevant records were excluded. Full texts were sought for the 149 remaining reports, of which 6 could not be retrieved. The 143 retrieved reports were assessed for eligibility, with 108 excluded for insufficient technical depth (n = 41), lack of healthcare focus (n = 37), methodological limitations (n = 18) or duplication of content already captured from related sources (n = 12). The inclusion phase yielded a final sample of 35 publications, combining seminal authors for theoretical grounding with recent publications for recency of technological and threat understanding.

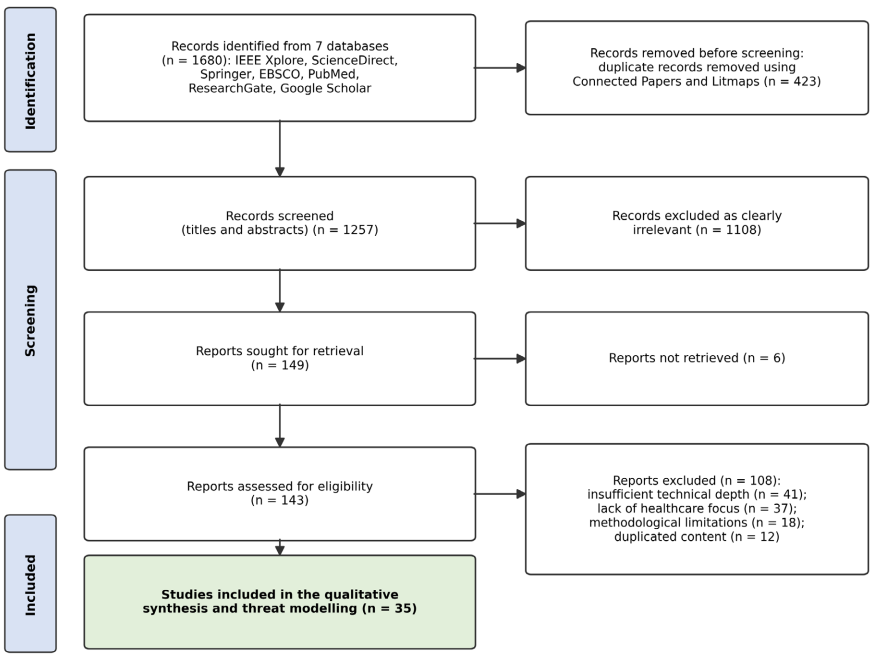

Figure 1. PRISMA 2020 flow diagram of the study selection process (adapted from Page *et al.*, 2021).

Data extraction. Each of the 35 included publications was read multiple times, with detailed information extracted into a structured extraction form organised by predetermined data items: bibliographic information; HIoT architecture components; security threats and vulnerabilities; STRIDE-LM categorisation; healthcare-specific considerations; methodological details; and key findings and contributions. Attention was focused on identifying consistencies and contradictions across publications. The use of secondary data was also supported by practical and ethical considerations: healthcare cybersecurity research involves sensitive information about vulnerabilities in critical systems, making primary data collection through penetration testing or vulnerability assessment of operational HIoT systems ethically problematic and potentially illegal without approval.

4.2. Design Science Research to Model the Threats

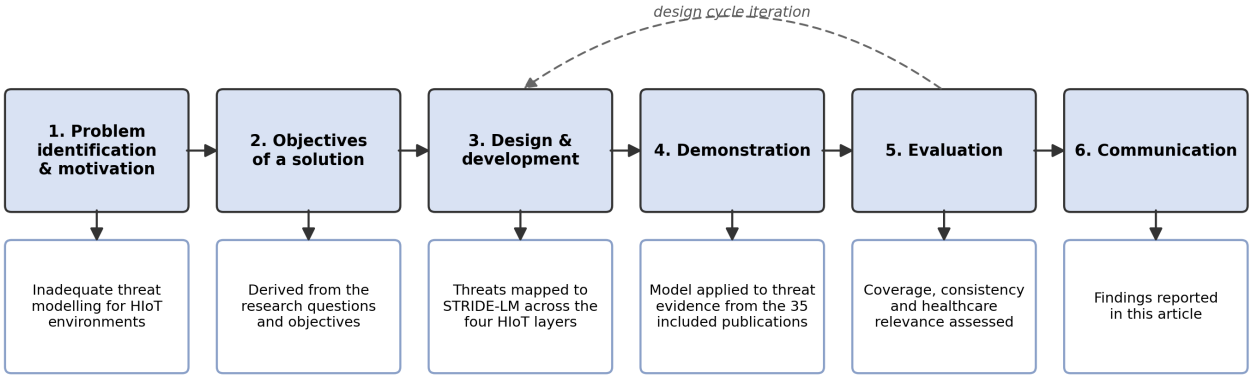

Figure 2. Design Science Research process for modelling HIoT threats (adapted from Peffers *et al.*, 2007).

The threats identified through the systematic review were modelled using the DSR methodology, which focuses on creating and evaluating IT artifacts intended to solve real-world problems [35]. The designed artifact of this research is the healthcare-adapted STRIDE-LM threat model, comprising the mapping of identified threats to the seven STRIDE-LM categories across the four HIoT architectural layers, together with the associated healthcare-specific considerations. The modelling followed the DSR process activities described by [36] as illustrated in **Figure 2**: 1) problem identification and motivation, established through the research problem of inadequate threat modelling for HIoT; 2) definition of objectives, derived from the research questions; 3) design and development, in which the threats extracted from the literature were categorised into the STRIDE-LM elements and distributed across the four architectural layers; 4) demonstration, applying the model to the threat evidence from the 35 publications; 5) evaluation, assessing coverage, consistency and healthcare relevance, with iteration back into design where gaps were identified; and 6) communication, realised through this article. Reference [37]'s three-cycle view further guided the research: the relevance cycle connected the artifact to the healthcare problem environment, the rigour

cycle grounded the artifact in the knowledge base assembled through the PRISMA-guided review, and the design cycle iterated between constructing the threat mappings and evaluating them against the literature.

4.3. Data Analysis

Within the design and development activity, the extracted data were analysed using thematic analysis and content analysis. Thematic analysis, the primary analytical method, followed six steps: familiarisation, categorising, theme development, theme review, theme refinement and reporting. Content analysis supported the thematic analysis by providing systematic categorisation of specific elements such as architectural components, threat types and STRIDE-LM categories, enabling quantitative description of qualitative data (for example, the frequency of threat types across the literature and the prevalence of specific vulnerabilities by architectural layer).

The analysis began with familiarisation through multiple readings of all extracted data. Systematic categorisation identified all references to architectural components, producing notes across four predetermined categories (Physical, Network, Processing and Application layers); the coding was both deductive (for example, "Physical Layer: wearable devices") and inductive (for example, "Physical Layer: implantable cardiac monitors"). Cybersecurity threats, vulnerabilities and attacks were then coded, organised primarily by affected architectural layer and attack type, distinguishing between general IoT threats and healthcare-specific threats. All threats were subsequently mapped to STRIDE-LM categories based on the definitions of [11] and categories were organised into themes representing broader patterns organised around the three research questions.

Comparative analysis across sources identified patterns in the literature. For instance, sources published before 2020 emphasised device-level vulnerabilities [2] while post-2020 sources increasingly highlighted system-level and integration vulnerabilities [27], a pattern suggesting an evolving threat landscape. Pattern identification also examined relationships between architectural layers and threat types, revealing that Physical Layer threats predominantly involved Tampering and Denial of Service, while Application Layer threats more frequently involved Information Disclosure and Elevation of Privilege.

4.4. Validity, Reliability, Ethics and Limitations

Trustworthiness was enhanced through triangulation of multiple data sources (peer-reviewed literature, technical documentation and industry reports), through the transparent and reproducible study selection process reported in accordance with PRISMA 2020 [33], and through clearly defined inclusion and exclusion criteria that maintained consistency in source selection. The use of established theoretical foundations and the structured DSR evaluation of the artifact further enhanced the rigor of the analysis.

Ethically, the modelling of threats using STRIDE-LM in HIoT revealed critical

security vulnerabilities that could potentially be exploited by malicious actors. The research therefore balanced transparency about security threats with the responsibility of not providing ways to attack vulnerable healthcare stakeholders, with special consideration for threats that could directly impact patient safety. Findings are communicated in a way that enables security improvements without compromising healthcare technologies.

Several limitations must be acknowledged. Without access to operational HIoT architectures for testing, the research could not validate the practical effectiveness of STRIDE-LM for detecting all real-world security threats, and it could not account for proprietary or classified HIoT architectures. The threat modelling was based on literature and therefore does not fully represent real-world implementations and differences in HIoT architecture, nor could it fully address organisational, cultural or human factors influencing security measures. Finally, the dynamically evolving nature of cybersecurity means new threats emerge frequently, and findings may require regular updates to maintain relevance.

5. Findings and Interpretation

The analysis of the 35 publications yielded findings systematically examining HIoT architectural components, cybersecurity threats and the application of STRIDE-LM threat modelling.

5.1. HIoT Architectural Components Identified

The analysis revealed a four-layer architectural model consistently described across the publications, with distinct component types identified at each layer. Table 3 presents the distribution of components across architectural layers.

Table 3. HIoT architectural components by layer.

Architectural layer	Component categories	Specific components identified
Physical Layer	Wearable devices, implantable devices, stationary medical equipment, environmental sensors	Cardiac monitors, glucose sensors, infusion pumps, ventilators, smart beds
Network Layer	Wireless protocols, wired connections, network infrastructure	Bluetooth Low Energy, Wi-Fi 6, ZigBee, LoRaWAN, 5G cellular
Processing Layer	Edge computing systems, cloud platforms, analytics engines	Healthcare-specific clouds, real-time analytics platforms
Application Layer	Electronic health records, patient portals, clinical decision support, remote monitoring applications	Telemedicine platforms, clinical dashboards, mobile health apps

At the Physical Layer, three primary device categories were identified: implantable devices (pacemakers, insulin pumps, neurostimulators), wearable sensors (fitness trackers, continuous glucose monitors, ECG monitors) and stationary medical equipment (infusion pumps, ventilators, imaging equipment). Critically, the publications noted that many medical devices operate with outdated firmware, with [19] claiming that healthcare facilities run firmware versions at least two

years old. The Network Layer demonstrated significant protocol diversity, with the most frequently mentioned protocols being Bluetooth Low Energy, Wi-Fi and ZigBee; [27] noted that healthcare facilities typically deploy multiple protocols simultaneously, and [22] reported that hospital networks lack proper segmentation, allowing potential attackers to access critical systems. The Processing Layer comprised data handling across edge computing, cloud processing and hybrid architectures. The Application Layer included healthcare-specific software systems, with Electronic Health Records systems mentioned most frequently, followed by remote patient monitoring platforms; [26] noted that most healthcare applications employ weak authentication methods.

Each architectural layer faces distinct security challenges that align with its functional characteristics. The Physical Layer confronts threats related to outdated firmware, device tampering and unauthorised data extraction; the Network Layer faces unencrypted Wi-Fi communications, DDoS attacks and signal interception; the Processing Layer encounters data manipulation, privilege escalation and weak access controls; and the Application Layer faces weak authentication mechanisms, ransomware attacks and poor session management. This layered view demonstrates the principle emphasized by [27] and [22] that HIoT security cannot be addressed through individual component protection but requires layer-specific strategies. Notably, some threats, such as weak authentication and access controls, span multiple layers, suggesting that certain security measures require implementation across the entire architectural system.

5.2. Cybersecurity Threat Categories in HIoT

The analysis identified distinct cybersecurity threat patterns across the 35 publications, organized into six thematic categories. **Table 4** summarises the primary threat categories.

Table 4. Cybersecurity threat categories in HIoT.

Threat category	Example threats	Affected layers
Patient data privacy breaches	Data transmission interception, database breaches	All layers
Device manipulation and tampering	Firmware modification, dosage alteration, sensor data manipulation	Physical and Processing layers
Service disruption and availability attacks	DDoS attacks, ransomware, device jamming, network flooding	All layers
Authentication and access control failures	Weak passwords, default credentials, privilege escalation, session hijacking	Application and Processing layers
Lateral movement and network propagation	Switching between systems, credential reuse, exploiting trust relationships	Network and Processing layers
Supply chain and lifecycle vulnerabilities	Compromised components, insecure updates, unsupported legacy devices	Physical layer, affects all layers

Patient data privacy breaches emerged as the most prominent threat. Reference [19] categorised privacy breaches into unauthorised database access, network traf-

fic interception and insider threats, while [14] emphasised that healthcare data breaches carry unique consequences including psychological distress, loss of trust and potential discrimination based on revealed health conditions.

Device manipulation and tampering threats were discussed with particular emphasis on life-critical risks. Reference [6] identified three primary categories: firmware manipulation, configuration tampering and sensor data manipulation. Several publications connected tampering threats to potential patient death, distinguishing HIoT from other IoT domains where consequences are typically limited to data integrity or financial loss.

Service disruption and availability attacks threaten healthcare delivery through DDoS attacks, ransomware and physical device modifications. Reference [33] emphasised that availability attacks can have immediate life-threatening consequences, and [32] noted that healthcare facilities accounted for 23% of all ransomware attacks in 2021 this is attributed to industry ransomware-incidents reporting for 2021, reflecting disclosed, sector-attributed incidents rather than a verified count of all attacks across the sector.

Authentication and access control failures enable unauthorised system access. Reference [26] identified weak password policies, default credentials, lack of multi-factor authentication, improper session management and inadequate access controls as primary weaknesses, reporting that most healthcare facilities lack robust authentication at the Processing Layer and employ weak authentication at the Application Layer.

Lateral movement and network propagation threats involve attackers leveraging initial access to expand across interconnected systems. Reference [13] described typical patterns: initial compromise of a vulnerable device, network reconnaissance, credential harvesting and progressive movement toward high-value systems, while [10] identified organisational factors facilitating lateral movement, including shared credentials and poor trust relationships.

Finally, supply chain and lifecycle vulnerabilities span the entire device lifecycle; [23] categorised these into design-phase vulnerabilities, manufacturing-phase compromises, deployment-phase weaknesses, operational-phase degradation and end-of-life risks. Publications noted that healthcare organisations frequently cannot patch medical devices due to regulatory constraints, compatibility concerns or vendor limitations.

5.3. STRIDE-LM Threat Modelling Application to HIoT

The systematic mapping of identified threats to STRIDE-LM elements revealed distinct patterns in how different threat types manifest across the architectural layers of HIoT, as shown in **Table 5**.

Spoofing threats involve identity misrepresentation at various architectural levels: device impersonation at the Physical Layer, protocol exploitation at the Network Layer, data source misrepresentation at the Processing Layer and user identity theft at the Application Layer. These threats are particularly concerning

healthcare contexts, where false device identities or data sources could result in inappropriate clinical interventions.

Table 5. STRIDE-LM threat distribution across HIoT architecture.

STRIDE-LM category	Physical Layer	Network Layer	Processing Layer	Application Layer	Primary healthcare considerations
Spoofing	Device impersonation	Protocol spoofing	Data source spoofing	User impersonation	False patient identities, altered medical devices affecting treatment
Tampering	Firmware modification	Man-in-the-middle	Data manipulation	Record alteration	Altered medication dosages, manipulated vital signs
Repudiation	Device activity logs absent	Network audit gaps	Processing trail incomplete	User action logging weak	Inability to trace medical errors
Information Disclosure	Sensor data exposure	Transmission interception	Processing leakage	Database breaches	Patient privacy breaches
Denial of Service	Device jamming	Network flooding	Resource exhaustion	Application overload	Critical care interruption, life-support unavailability
Elevation of Privilege	Device admin access	Network infrastructure control	Middleware escalation	Application admin rights	Unauthorised access to medication systems, clinical overrides
Lateral Movement	Device-to-device propagation	Network traversal	Cross-system pivoting	Application movement	Hospital-wide compromise, multi-patient data exposure

Tampering threats attracted particular attention due to their patient safety implications. Reference [6] and [13] provided examples including altered insulin pump dosing algorithms and modified pacemaker pacing rates, all with potentially lethal consequences. Publications addressing tampering emphasised that this category presents the most severe patient safety risks, distinguishing healthcare from other IoT domains.

Repudiation threats received the least attention yet remain important. Reference [31] and [6] highlighted that inadequate logging creates forensic and auditing challenges; in healthcare contexts, repudiation threats undermine accountability for clinical actions and can delay investigations following security incidents or adverse patient outcomes.

Information Disclosure threats were the most frequently mentioned STRIDE-LM category, reflecting widespread concern about patient data privacy, from unauthorised sensor data access at the Physical Layer through transmission interception and processing leakage to database breaches at the Application Layer. Healthcare-specific considerations include regulatory compliance requirements, the unique sensitivity of health information and the potential for discrimination [38].

Denial of Service threats compromise healthcare availability, manifesting as wireless jamming, network flooding, resource exhaustion and application overload across the layers. Sources emphasised that DoS attacks in healthcare can directly threaten patient safety by delaying critical care delivery, preventing access to medication systems or disrupting life-support device communications [38].

Elevation of Privilege threats involve attackers gaining unauthorised access rights, from administrative device access at the Physical Layer to unauthorised administrative access to clinical applications. Reference [26] reported that many healthcare applications employ inadequate access controls which attackers can capitalise on to gain access to healthcare systems and elevate their privilege to further damage the systems. Elevated privileges could enable unauthorised access to medication systems, patient records or clinical decision-support systems.

Lateral Movement addresses attackers' ability to expand their presence after initial compromise. Sources emphasised that a lack of proper network segmentation facilitates lateral movement across HIoT systems; the healthcare-specific concern is that lateral movement can transform isolated device compromises into hospital-wide system failures affecting multiple patients simultaneously [39].

Different architectural layers present distinct threat profiles: the Physical Layer faces predominantly Tampering and Denial of Service, the Network Layer shows a focus on Information Disclosure and Spoofing, the Processing Layer demonstrates a balanced threat distribution, and the Application Layer heavily emphasises Information Disclosure and Elevation of Privilege. This suggests that security strategies should be tailored to the threats at each layer.

5.4. Implementation Gaps and Interpretation

A striking pattern emerged where sources acknowledged threats yet reported widespread mitigation failure. For example, sources emphasised the importance of encryption, yet [19] reported that many communications in HIoT remain unencrypted. This implementation gap suggests technical knowledge is necessary but insufficient for security adoption. While sources identify specific vulnerabilities like unencrypted communications and outdated firmware [19] and inadequate network segmentation [22], they provide limited explanation for why these vulnerabilities persist despite widespread awareness. The analysis identified several contributing factors.

First, the regulatory environment creates constraints in which device manufacturers cannot easily update firmware without risking violations of regulatory approvals, forcing healthcare organisations to choose between compliance with existing device approvals and implementing security patches. Second, healthcare organisations operate under severe resource constraints where security investments compete directly with clinical care priorities, creating underinvestment despite threat awareness. Third, the interconnected nature of HIoT means robust security requires action across multiple stakeholders, *i.e.* device manufacturers, healthcare IT departments, clinical staff, regulators and healthcare providers, and a failure at any point compromises the entire system: secure devices may be deployed on inadequately segmented networks, clinicians may disable authentication measures to expedite emergency care, and regulators may demand standards while lacking enforcement methods.

The finding that Tampering threats present potentially lethal consequences yet

receive less systematic attention than Information Disclosure threats reveals a fundamental misalignment between security prioritisation and patient safety needs. Regulations emphasise patient data privacy, creating strong incentives to invest in preventing information disclosure, whereas tampering threats that could directly harm patients lack equivalent regulatory attention. This aligns with the Protection Motivation Theory, suggesting that regulatory enforcement creates stronger protection motivation for privacy than for potentially more severe tampering threats. Similarly, from a Technology Threat Avoidance Theory perspective [17], the obscurity of repudiation threats may reduce their perceived severity, leading to inadequate countermeasures. The broader implementation gap invites interpretation through the Theory of Planned Behaviour [18], *i.e.* healthcare organisations possess positive security attitudes, for example threat awareness, but lack either organisational prioritisation or adequate perceived behavioural control like resources and capabilities, suggesting that closing implementation gaps requires addressing organisational culture and resource allocation. However, none of these theories directly addresses the unique ethical concern that failures may cause patient harm, suggesting a need for healthcare-specific theoretical adaptations.

The identification of lateral movement as a significant threat category, facilitated by inadequate network segmentation [22], reveals how IT infrastructure decisions create vulnerabilities: many facilities designed their networks when medical devices required minimal connectivity, and the incremental integration of these devices into HIoT occurred without network redesign, creating architectures where devices at different trust levels share network segments. Furthermore, medical devices operate for extended periods that far exceed typical technology lifecycles: devices deployed with adequate security may become critically vulnerable years later as attack techniques evolve, encryption standards deprecate or vendor support ends. Sustainable security in HIoT therefore requires not only initial deployment security but lifecycle security management.

Finally, the findings indicate that STRIDE-LM, when appropriately adapted for healthcare, provides comprehensive literature-based coverage of HIoT threats. The present study establishes this coverage against the reviewed literature rather than demonstrating operational effectiveness, which remains to be validated against real world deployments. The seven categories enable comprehensive threat identification, reducing the risk of overlooking significant vulnerabilities; the layer-by-layer analysis approach aligns naturally with HIoT's layered architecture, enabling structured security assessment; and the incorporation of Lateral Movement as a distinct category addresses the interconnected nature of healthcare systems where initial compromises can spread across networks.

5.5. Healthcare-Specific Assessment Criteria

Adapting STRIDE-LM to healthcare required more than mapping threats to the seven categories; each mapped threat was additionally assessed against four explicit, healthcare-specific criteria derived from the reviewed literature [6] [22]

[31]. These criteria, defined in Table 6, distinguish healthcare threat modelling from generic STRIDE-LM application by foregrounding consequences for patients and the operational realities of clinical environments. Each criterion was rated on a three-point ordinal scale (Low, Medium, High) to support the prioritisation described in Section 5.5.2.

Table 6. Healthcare-specific assessment criteria applied to each mapped threat.

Criterion	Definition	Rating anchors (High/Medium/Low)
Patient-safety impact	The degree to which exploitation could cause direct physical harm to a patient (e.g. altered dosing, disabled monitoring, disrupted life support).	High: plausible loss of life or serious injury; Medium: treatment delay or degraded care; Low: no direct clinical harm.
Clinical criticality	The importance of the affected device or system to active clinical workflows and continuity of care.	High: life-supporting or time-critical system; Medium: important but with clinical fallback; Low: administrative or non-clinical.
Regulatory constraints	The extent to which approval or compliance obligations limit or complicate mitigation (e.g. firmware locked by device certification; data-handling duties under HIPAA/GDPR).	High: mitigation blocked or heavily constrained by approval regimes; Medium: mitigation permitted with compliance overhead; Low: no material regulatory barrier.
Device lifecycle status	The maturity and supportability of the affected device across its service life.	High: end-of-life, unsupported or legacy device; Medium: supported but ageing; Low: current, actively maintained.

5.5.1. Threat Prioritisation

Mapping a threat to a STRIDE-LM category records its nature but not its urgency. To make prioritisation explicit, each mapped threat was assigned a priority tier derived from its four criterion ratings. Because harm to patients is the distinguishing concern of healthcare applicants, patient-safety impact and clinical criticality were treated as dominant criteria: a High rating on either was sufficient to place a threat in at least the High tier, irrespective of exploitation likelihood. Regulatory constraints and device lifecycle status acted as escalating modifiers, raising a threat's tier where they indicated that mitigation would be delayed or infeasible for example, a tampering threat on an end-of-life, certification-locked infusion pump. The resulting four-tier scheme is summarised in Table 7.

Table 7. Threat prioritisation scheme applied after STRIDE-LM classification.

Priority tier	Assignment rule	Illustrative STRIDE-LM threats
Critical	High patient-safety impact AND (High clinical criticality OR mitigation blocked by regulatory or lifecycle constraints).	Tampering with infusion-pump or pacemaker firmware; Denial of Service against life-support communications.
High	High patient-safety impact OR High clinical criticality, with mitigation feasible.	Lateral Movement across unsegmented clinical networks; Elevation of Privilege on medication-administration systems.
Medium	Medium patient-safety impact or criticality; consequences primarily affect data confidentiality.	Information Disclosure of stored records; Spoofing of non-critical data sources.
Low	Low patient-safety impact and criticality; administrative or non-clinical exposure.	Repudiation gaps in non-clinical logging; disclosure of non-sensitive telemetry.

Applying this scheme to the mapped threats placed Tampering and Denial of Service at the Physical and Network layers, together with Lateral Movement, in the Critical and High tiers, whereas Information Disclosure and Repudiation threats; despite their frequency in the literature more often occupied the Medium and Low tiers. This ordering is a property of the literature-derived model and its criteria, not an empirically measured risk ranking.

5.5.2. Evaluation Criteria and Outcomes

The DSR evaluation activity assessed the artifact against three criteria, each with an explicit definition, an assessment method and a reported outcome, as summarised in Table 8. The evaluation was formative and literature-based *i.e.* the artifact was evaluated against the body of evidence used to construct it, so the outcomes establish internal coverage, consistency and healthcare relevance rather than operational performance in a real-world healthcare environment.

Table 8. DSR evaluation criteria, methods and outcomes.

Criterion	Definition and assessment method	Evaluation outcome
Coverage	Whether every STRIDE-LM category is populated across every HIoT layer and whether the threats extracted from the 35 sources map without unclassifiable residuals. Assessed by a completeness check of the layer-by-category matrix in Table 4.	Achieved: all seven categories were populated across all four layers, and every extracted threat mapped to at least one category, with no unclassifiable residual threats.
Consistency	Whether identical or equivalent threats from different sources receive the same category and layer assignment. Assessed by cross-source comparison of repeated threats and reconciliation against the definitions in [11].	Substantially achieved: mappings agreed for the majority of repeated threats; a small number of boundary cases (notably Elevation of Privilege versus Lateral Movement) were reconciled by returning to the source definitions and re-coding.
Healthcare relevance	Whether each mapped category is tied to a concrete healthcare consequence and to the criteria of Section 4.2.1. Assessed by requiring, for each category, at least one documented patient-safety or clinical-operations implication from the literature.	Achieved: each category was linked to at least one healthcare-specific consequence (e.g. Tampering to altered dosing; Denial of Service to interrupted critical care), as reflected in the healthcare-considerations column of Table 4.

These outcomes should be read as evidence of literature-based coverage, consistency and relevance. They do not, and on this evidence base cannot, demonstrate operational effectiveness, which would require evaluating the artifact against real-world HIoT deployments.

6. Reflecting on the Research Questions

Regarding the first research question, the research identified a four-layer architectural model consisting of distinct HIoT component types across the Physical, Network, Processing and Application layers. The Physical Layer encompasses device types (implantable devices, wearables, stationary equipment), the Network Layer comprises communication protocols, the Processing Layer includes processing system types, and the Application Layer encompasses software systems.

Critically, the research revealed that vulnerabilities frequently emerge at integration points between layers rather than within individual components, emphasising that security in HIoT requires architectural understanding.

Regarding the second research question, the research identified distinct cybersecurity threat patterns organized into six thematic categories covering all of the STRIDE-LM classifications: patient data privacy breaches, device manipulation and tampering, service disruption, authentication failures, lateral movement and supply chain vulnerabilities. Critically, HIoT threats differ substantially from general IoT threats in their life-critical consequences, where threats can directly cause patient harm through manipulated device settings, altered medication dosages or disrupted life-support systems. The research also revealed significant implementation gaps where vulnerabilities persist despite widespread awareness: unencrypted communications, outdated firmware, weak authentication and inadequate network segmentation.

Regarding the third research question, the research demonstrated the application of STRIDE-LM as a technique for HIoT threat modelling when adapted to healthcare contexts. The seven categories successfully incorporate the identified threats, and the application methodology requires architectural documentation, systematic threat examination, healthcare-specific impact assessment, attack chain analysis and priority determination. Critical healthcare-specific adaptations include incorporating patient safety impact assessment, integrating regulatory compliance considerations, accounting for operational constraints, addressing extended device lifecycles and recognising implementation barriers.

Collectively, these findings directly address the research problem of inadequate security measures and threat modelling techniques by demonstrating how adapting STRIDE-LM to healthcare contexts provides threat identification across seven categories and all architectural layers. The documentation of implementation gaps validates that the inadequacy arises from systemic challenges preventing implementation rather than a shortage of knowledge. The research provides healthcare stakeholders with architectural models, threat analysis and systematic approaches for security assessments, though actual security improvement depends on stakeholders utilising these insights to affect organisational and technical change.

7. Conclusion

This research addressed a critical gap in cybersecurity understanding within Healthcare Internet of Things (HIoT) environments by applying the STRIDE-LM threat modelling technique to healthcare contexts. Through the analysis of 35 peer-reviewed publications, the research identified architectural components, categorised cybersecurity threats and demonstrated the application of STRIDE-LM for modelling threats specific to healthcare environments. The research established that HIoT operates through a four-layer architectural model consisting of Physical, Network, Processing and Application layers, each presenting distinct security vulnerabilities requiring targeted mitigation strategies. The systematic cat-

egorisation of threats across the seven STRIDE-LM categories of Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege and Lateral Movement revealed that HIoT security challenges fundamentally differ from other IoT domains due to the implications for patient safety and the life-critical nature of healthcare operations. The research therefore demonstrated that STRIDE-LM, when appropriately adapted for healthcare contexts, provides comprehensive, literature-based coverage for threat identification and modelling across all architectural layers in HIoT. This coverage was established against the reviewed literature; operational effectiveness in live healthcare settings was not evaluated and remains an item for future work. Future work should validate the adapted technique against operational healthcare deployments and investigate the organisational and regulatory interventions needed to close the implementation gaps identified in this research.

Author Contributions

Conceptualization, A.M.; methodology, A.M.; validation, B.M.; formal analysis, A.M., B.M.; investigation, A.M.; resources, A.M.; writing—original draft preparation, A.M., B.M.; writing—review and editing, A.M., B.M.; visualization, A.M.; supervision, B.M.; funding acquisition, A.M. All authors have read and agreed to the published version of the manuscript.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Affia, A.O., Finch, H., Jung, W., Samori, I.A., Potter, L. and Palmer, X. (2023) IoT Health Devices: Exploring Security Risks in the Connected Landscape. *IoT*, **4**, 150-182. https://doi.org/10.3390/iot4020009

[2] Aijaz, M., Nazir, M. and Mohammad, M.N.A. (2023) Threat Modeling and Assessment Methods in the Healthcare-It System: A Critical Review and Systematic Evaluation. *SN Computer Science*, **4**, Article No. 714. https://doi.org/10.1007/s42979-023-02221-1

[3] Ajzen, I. (1991) The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, **50**, 179-211. https://doi.org/10.1016/0749-5978(91)90020-t

[4] Baker, S.B., Xiang, W. and Atkinson, I. (2017) Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access*, **5**, 26521-26544. https://doi.org/10.1109/access.2017.2775180

[5] Cagnazzo, M., Hertlein, M., Holz, T. and Pohlmann, N. (2018) Threat Modeling for Mobile Health Systems. 2018 *IEEE Wireless Communications and Networking Conference Workshops* (*WCNCW*), Barcelona, 15-18 April 2018, 314-319. https://doi.org/10.1109/wncnw.2018.8369033

[6] Dwivedi, R., Mehrotra, D. and Chandra, S. (2022) Potential of Internet of Medical Things (IoMT) Applications in Building a Smart Healthcare System: A Systematic Review. *Journal of Oral Biology and Craniofacial Research*, **12**, 302-318. https://doi.org/10.1016/j.jobcr.2021.11.010

[7] Ewoh, P. and Vartiainen, T. (2024) Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. *Journal of Medical Internet Research*, **26**, e46904. https://doi.org/10.2196/46904

[8] Haag, S., Siponen, M. and Liu, F. (2021) Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, **52**, 25-67. https://doi.org/10.1145/3462766.3462770

[9] Hasan, M.K., Ghazal, T.M., Saeed, R.A., Pandey, B., Gohel, H., Eshmawi, A.A., *et al.* (2021) A Review on Security Threats, Vulnerabilities, and Counter Measures of 5G Enabled Internet-of-Medical-Things. *IET Communications*, **16**, 421-432. https://doi.org/10.1049/cmu2.12301

[10] Hevner, A.R. (2007) A Three Cycle View of Design Science Research. Scandinavian *Journal of Information Systems*, **19**, Article 4.

[11] Hevner, A. and Chatterjee, S. (2010) Design Science Research in Information Systems. In: Hevner, A. and Chatterjee, S., Eds., *Design Research in Information Systems*, Springer, 9-22. https://doi.org/10.1007/978-1-4419-5653-8_2

[12] Kamalov, F., Pourghebleh, B., Gheisari, M., Liu, Y. and Moussa, S. (2023) Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective. *Sustainability*, **15**, Article 3317. https://doi.org/10.3390/su15043317

[13] Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S., *et al.* (2023) Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. *Electronics*, **12**, Article 2050. https://doi.org/10.3390/electronics12092050

[14] Li, C., Wang, J., Wang, S. and Zhang, Y. (2024) A Review of IoT Applications in Healthcare. *Neurocomputing*, **565**, Article ID: 127017. https://doi.org/10.1016/j.neucom.2023.127017

[15] Li, N., Xu, M., Li, Q., Liu, J., Bao, S., Li, Y., *et al.* (2023) A Review of Security Issues and Solutions for Precision Health in Internet-of-Medical-Things Systems. *Security and Safety*, **2**, Article ID: 2022010. https://doi.org/10.1051/sands/2022010

[16] Liang, H. and Xue, Y. (2009) Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, **33**, 71-90. https://doi.org/10.2307/20650279

[17] López Martínez, A., Gil Pérez, M. and Ruiz-Martínez, A. (2023) A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare. *ACM Computing Surveys*, **55**, 1-38. https://doi.org/10.1145/3571156

[18] Madanian, S., Chinbat, T., Subasinghage, M., Airehrour, D., Hassandoust, F. and Yongchareon, S. (2024) Health IoT Threats: Survey of Risks and Vulnerabilities. *Future Internet*, **16**, Article 389. https://doi.org/10.3390/fi16110389

[19] Maodza, B. and du Toit, J. (2024) Agricultural Internet of Things (AIoTs) Threat Modeling Using Stride-LM. In: Yang, X.S., Sherratt, S., Dey, N. and Joshi, A., Eds., *Proceedings of Ninth International Congress on Information and Communication Technology*, Springer, 295-312. https://doi.org/10.1007/978-981-97-3302-6_24

[20] Nasiri, S., Sadoughi, F., Tadayon, M. and Dehnad, A. (2019) Security Requirements of Internet of Things-Based Healthcare System: A Survey Study. *Acta Informatica Medica*, **27**, 253-258. https://doi.org/10.5455/aim.2019.27.253-258

[21] Newaz, A.I., Sikder, A.K., Rahman, M.A. and Uluagac, A.S. (2021) A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses. *ACM Transactions on Computing for Healthcare*, **2**, 1-44. https://doi.org/10.1145/3453176

[22] Nurse, J.R.C., Creese, S. and De Roure, D. (2017) Security Risk Assessment in Internet of Things Systems. *IT Professional*, **19**, 20-26. https://doi.org/10.1109/mitp.2017.3680959

[23] Omotosho, A., Ayemlo Haruna, B. and Mikail Olaniyi, O. (2019) Threat Modeling of Internet of Things Health Devices. *Journal of Applied Security Research*, **14**, 106-121. https://doi.org/10.1080/19361610.2019.1545278

[24] Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., *et al.* (2021) The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ*, **372**, n71. https://doi.org/10.1136/bmj.n71

[25] Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007) A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, **24**, 45-77. https://doi.org/10.2753/mis0742-1222240302

[26] Pfleeger, C.P., Pfleeger, S.L. and Margulies, J. (2015) Security in Computing. 5th Edition, Prentice Hall.

[27] Qadri, Y.A., Nauman, A., Zikria, Y.B., Vasilakos, A.V. and Kim, S.W. (2020) The Future of Healthcare Internet of Things: A Survey of Emerging Technologies. *IEEE Communications Surveys & Tutorials*, **22**, 1121-1167. https://doi.org/10.1109/comst.2020.2973314

[28] Qureshi, R. and Koo, I. (2026) A Comprehensive Survey of Cybersecurity Threats and Data Privacy Issues in Healthcare Systems. *Applied Sciences*, **16**, Article 1511. https://doi.org/10.3390/app16031511

[29] Salih, F.I., Abu Bakar, N.A., Hassan, N.H., Yahya, F., Kama, N. and Shah, J. (2019) IoT Security Risk Management Model for Healthcare Industry. *Malaysian Journal of Computer Science*, No. 3, 131-144. https://doi.org/10.22452/mjcs.sp2019no3.9

[30] Scandariato, R., Wuyts, K. and Joosen, W. (2015) A Descriptive Study of Microsoft's Threat Modeling Technique. *Requirements Engineering*, **20**, 163-180. https://doi.org/10.1007/s00766-013-0195-2

[31] Selvaraj, S. and Sundaravaradhan, S. (2020) Challenges and Opportunities in IoT Healthcare Systems: A Systematic Review. *SN Applied Sciences*, **2**, Article No. 139. https://doi.org/10.1007/s42452-019-1925-y

[32] Shahid, J., Ahmad, R., Kiani, A.K., Ahmad, T., Saeed, S. and Almuhaideb, A.M. (2022) Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Applied Sciences*, **12**, Article 1927. https://doi.org/10.3390/app12041927

[33] Shostack, A. (2014) Threat Modeling: Designing for Security. John Wiley & Sons.

[34] Tariq, U., Ahmed, I., Bashir, A.K. and Shaukat, K. (2023) A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, **23**, Article 4117. https://doi.org/10.3390/s23084117

[35] Vallabhaneni, R. and Veeramachaneni, V. (2024) Threat Modeling for Enhanced Security in the Healthcare Industry with a Focus on Mobile Health and IoT. *Engineering and Technology Journal*, **9**, 5329-5331. https://doi.org/10.47191/etj/v9i10.10

[36] Vilakazi, K. and Adebesin, F. (2023) A Systematic Literature Review on Cybersecurity Threats to Healthcare Data and Mitigation Strategies. *Proceedings of the Conference on Information Communications Technology and Society*, Durban, 8-9 March 2023, 240-251.

[37] vom Brocke, J., Hevner, A. and Maedche, A. (2020) Introduction to Design Science Research. In: vom Brocke, J., Hevner, A. and Maedche, A., Eds., *Design Science Research. Cases*, Springer, 1-13. https://doi.org/10.1007/978-3-030-46781-4_1

[38] Williams, P., Dutta, I.K., Daoud, H. and Bayoumi, M. (2022) A Survey on Security in Internet of Things with a Focus on the Impact of Emerging Technologies. *Internet of Things*, **19**, Article ID: 100564. https://doi.org/10.1016/j.iot.2022.100564

[39] Xiong, W. and Lagerström, R. (2019) Threat Modeling—A Systematic Literature Review. *Computers & Security*, **84**, 53-69. https://doi.org/10.1016/j.cose.2019.03.010