

# A Knowledge-driven, AI-assisted Cyber Defence Framework for IoMT Remote Patient Monitoring

Kulsoom S. Bughio<sup>1</sup>, David M. Cook<sup>1</sup> and Abdul M. Unar<sup>2</sup>

<sup>1</sup>Edith Cowan University, Joondalup, Western Australia, Australia

<sup>2</sup>Mehran University of Engineering and Technology, Jamshoro, Pakistan

[k.bughio@ecu.edu.au](mailto:k.bughio@ecu.edu.au)

[d.cook@ecu.edu.au](mailto:d.cook@ecu.edu.au)

[majeedunar@gmail.com](mailto:majeedunar@gmail.com)

**Abstract:** The rapid adoption of Internet Medical Things (IoMT) technologies in remote patient monitoring has reshaped healthcare delivery by enabling continuous, real-time clinical observation outside traditional care settings. However, this shift has also expanded the cyber-attack surface across heterogeneous, resource-constrained medical devices, wireless networks, cloud services, and third-party platforms. In cyber warfare, healthcare has become an incorporated target of geopolitics, with hospitals, remote monitoring systems, and emergency health systems being used to broaden the attack surface for adversaries to exploit. Existing security approaches for IoMT environments remain largely manual, fragmented, and reactive, limiting their effectiveness in dynamically assessing vulnerabilities and supporting timely defensive decision-making. In critical healthcare contexts, such limitations pose direct risks to patient safety, data integrity, and system availability. This research proposes a knowledge-driven methodology pipeline for semantic reasoning and partial automation to strengthen cyber defence in IoMT-enabled remote patient monitoring systems. The pipeline integrates domain ontologies, rule-based reasoning, and knowledge graph representation to formally model medical devices, vulnerabilities, attack vectors, potential cyber-physical impacts, and mitigation strategies. By structuring and linking heterogeneous security knowledge with external cyber threat intelligence, the proposed approach enables context-aware vulnerability detection, automated inference, and explainable security insights. The methodology follows a science and engineering research design, progressing from conceptual modelling to prototype development, semantic framework implementation, and validation. A vulnerability detection algorithm operationalizes the pipeline by systematically identifying exploitable weaknesses, assessing severity and impact, and recommending countermeasures through semantic queries and reasoning. Evaluation using representative remote patient monitoring scenarios demonstrates improved consistency, visibility, and timeliness in vulnerability identification compared to existing IoMT security frameworks. This work contributes to a practical, extensible, and automation-oriented semantic pipeline that enhances cyber resilience in healthcare systems considered part of the critical national infrastructure.

**Keywords:** Internet of medical things (IoMT), Healthcare cyber resilience, Vulnerability detection, Semantic cybersecurity framework, Cybersecurity governance

## 1. Introduction

With the evolution of IoT (Alsabah et al., 2025), WSNs (Ojha & Gupta, 2025) have become central to the development of real-time, data-driven healthcare solutions, supporting continuous patient monitoring, environmental sensing, and intelligent decision-making in modern smart healthcare systems. These technological advances have facilitated the creation of smart healthcare environments that support continuous monitoring, timely intervention, and improved quality of care, particularly for individuals living independently or managing chronic conditions (Alam Efat, 2025). Such environments are increasingly relied upon to provide safe and monitored living spaces in which health data can be collected, transmitted, and analysed by healthcare providers, allowing early detection of medical anomalies and timely clinical response.

Healthcare systems have increasingly become deliberate targets during armed conflict and geopolitical confrontation, transforming hospitals, emergency response networks, and remote patient monitoring (RPM) platforms into components of contested digital terrain. IoMT-enabled RPM systems extend clinical infrastructure into homes and community settings, creating a distributed attack surface that adversaries can exploit to degrade care continuity without physically striking hospitals. In this context, the proposed governance-aware semantic cyber defence framework offers strategic benefit by enabling early detection of vulnerabilities across interconnected medical devices, cloud services, and communication layers. By integrating knowledge graphs, rule-based reasoning, and regulatory control mapping, the framework enhances situational awareness not only at the technical level but also at the institutional governance level.

This is particularly important in wartime conditions where operational tempo increases, patch cycles are compressed, and device supply chains may be disrupted. A semantic model that links vulnerabilities to cyber-physical risk and compliance obligations enables healthcare providers to prioritize defensive actions in alignment with national resilience objectives. Rather than responding reactively to incidents, healthcare organizations can

proactively model cascading effects, such as compromised telemetry data influencing clinical decision-making. This reduces the probability that cyber interference escalates into clinical harm during periods of heightened geopolitical instability.

A specifically relevant adversary in this context is the hybrid actor. This type of actor is either a state-sponsored advanced persistent threat (APT) group or a ransomware organization operating with tacit state tolerance, seeking to generate coercive pressure without triggering overt military escalation (Deb, 2025). For example, during the Russia–Ukraine conflict, multiple cyber campaigns have targeted Ukrainian healthcare institutions and digital infrastructure, while ransomware groups such as Conti publicly aligned themselves with geopolitical objectives (Hansel & Silomon, 2024; Kapsokoli, 2025). In such scenarios, disruption of RPM networks could undermine chronic disease management, overload emergency departments, and erode civilian confidence in state capacity, thereby achieving strategic psychological and societal impact. A semantic, knowledge-driven defence architecture as proposed in this paper directly addresses this threat model by enabling traceable reasoning from exploited vulnerability to patient safety risk and governance escalation. By mapping device-level weaknesses to national cybersecurity frameworks and critical infrastructure oversight mechanisms, the framework strengthens healthcare cyber resilience against adversaries whose objectives extend beyond financial gain toward destabilization, coercion, or hybrid warfare. In a global environment where cyber operations increasingly accompany conventional conflict, embedding explainable, governance-aligned automation into IoMT ecosystems becomes not merely a technical improvement but a strategic necessity for protecting civilian populations and maintaining national stability (Ewoh & Vartiainen, 2024).

Within this context, the Internet of Medical Things (IoMT) has emerged as a critical enabling of connected healthcare. IoMT represents a specialized subset of the Internet of Things, integrating medical devices, sensors, actuators, and communication technologies to support patient monitoring, diagnosis, and treatment (SriPriyanka and Mahendran, 2021; Pritika, Shanmugam and Azam, 2023). These systems employ a wide range of devices, including wearable sensors, smart medical equipment, mobile applications, and cloud-based services, to enable continuous data exchange between patients, healthcare professionals, and service providers. Remote patient monitoring (RPM) systems allow patients to remain in their homes while clinicians receive real-time physiological data, supporting proactive and personalized care delivery (Bughio, 2023).

Despite these benefits, the increasing reliance on IoMT technologies introduces significant cybersecurity challenges. IoMT ecosystems are inherently heterogeneous, distributed, and resource-constrained, often lacking consistent security standards across devices, vendors, and deployment environments (Shah, 2026). Medical devices frequently rely on wireless communication technologies such as Bluetooth and Wi-Fi and transmit sensitive health data through cloud infrastructures, increasing exposure to cyber threats. Vulnerabilities within these systems can be exploited to compromise device functionality, manipulate medical data, violate patient privacy, or disrupt healthcare services, with potentially severe clinical consequences. Maintaining cyber resilience in IoMT-enabled healthcare systems is therefore a critical challenge. Traditional security approaches, which often rely on manual vulnerability assessment and isolated security controls, struggle to cope with the scale, complexity, and dynamic nature of IoMT environments. There is a growing need for structured, automated, and explainable security solutions capable of integrating heterogeneous security knowledge, identifying vulnerabilities in context, and supporting informed defensive decision-making (Bughio et al., 2024b; Ullah et al., 2025).

Beyond technical vulnerabilities, IoMT-enabled remote patient monitoring systems must be understood within the broader strategic context of critical healthcare infrastructure. As healthcare systems increasingly depend on interconnected medical devices and cloud-based services, cyber incidents no longer represent isolated technical failures but strategic risks affecting national resilience, public trust, and patient safety. Consequently, vulnerability detection mechanisms must support not only operational security teams but also governance, compliance, and policy-level decision-making. A knowledge-driven and explainable security framework enables strategic visibility across device ecosystems, supporting risk-informed resource allocation, regulatory compliance, and coordinated cyber defence at institutional and national levels. This research addresses this need by proposing a semantic framework designed to enhance the security posture of IoMT-based remote patient monitoring systems through partial automation, knowledge integration, and reasoning. By leveraging semantic technologies, rule-based reasoning, and knowledge graphs, the framework aims to support systematic vulnerability detection, impact assessment, and mitigation planning within healthcare environments considered part of critical national infrastructure.

This paper extends our prior work on conceptual modelling, ontology development, and preliminary semantic framework design (Buglio et al., 2024a; 2024b; 2024c) by introducing a governance-aware semantic cyber defence framework for IoMT-enabled remote patient monitoring systems. Unlike existing approaches that primarily focus on technical vulnerability detection, this research integrates cybersecurity analysis with institutional governance and regulatory compliance. The main contributions of this paper are as follows:

- A governance-aware vulnerability detection algorithm that formalizes the relationship between vulnerabilities, potential attacks, adverse cyber-physical impacts, and mitigation strategies, while incorporating risk classification and regulatory control mapping.
- An enhanced semantic framework that embeds governance-aware reasoning within an ontology-driven architecture, enabling automated, explainable, and context-aware vulnerability analysis.
- Integration of regulatory compliance and risk categorisation into the vulnerability detection lifecycle, providing traceability between technical security events and frameworks such as NIST Cybersecurity Framework and ISO/IEC 27001.
- A knowledge graph-based implementation that supports semantic querying, reasoning, and visualization of IoMT security insights for both technical and strategic decision-making.

By bridging semantic automation with cybersecurity governance, this work advances IoMT security from isolated technical detection toward a structured, explainable, and policy-aligned cyber defence capability.

## 2. Research Methodology and Design

In the field of computer science, researchers employ various methods to conduct their experiments. Broadly, these methods fall into two main categories: the scientific method and the mathematical method (Basili, 1993; Kelly, 2008). The scientific method, often regarded as the optimal paradigm for understanding software processes, products, people, and environments, involves observing the world, proposing models, measuring, analysing, and validating these models. It is subdivided into two approaches: the empirical method and the engineering method. This research adopts the scientific approach, specifically focusing on the engineering method subcategory. Research grounded in science and engineering enables researchers to validate theoretical predictions (Kelly, 2008). In this regard, researchers often propose solutions to problems by developing, measuring, and analysing techniques, methodologies, models, algorithms, or frameworks against existing solutions. In the engineering domain, the fundamental goal of 'creating functional solutions' is realized through three distinct levels, as identified by: *the conceptual level, the perceptual level, and the practical level*. Each of these levels is further elaborated as:

- a) **Conceptual Level:** At this initial stage, innovative ideas are formulated, leading to the creation of new concepts. This process involves a detailed analysis of the problem at hand.
- b) **Perceptual Level:** This level involves the development of new techniques based on novel approaches. It encompasses the design and development of specific tools, environments, or appropriate systems through implementation.
- c) **Practical Level:** At this final stage, the focus shifts to the application of testing and validation techniques. Experimentation is conducted based on real-world scenarios, employing either laboratory or testing methods are used.

This research focuses on developing a semantic framework designed to facilitate partial automation and enhance the security posture of IoT networks used in remote patient monitoring systems. At the core of this framework is a domain ontology that encapsulates the semantics of the concepts and properties critical to the main security aspects of IoT medical devices utilized in such systems. This ontology is augmented with a comprehensive ruleset, complex queries, and mechanisms that enable automated reasoning over aggregated knowledge. Consequently, to address the various tasks required to develop a solution, the science and engineering research methodology has been adopted as the primary research method. *Figure 1.* shows the research pipeline based on the Science and Engineering research methodology for this research work.

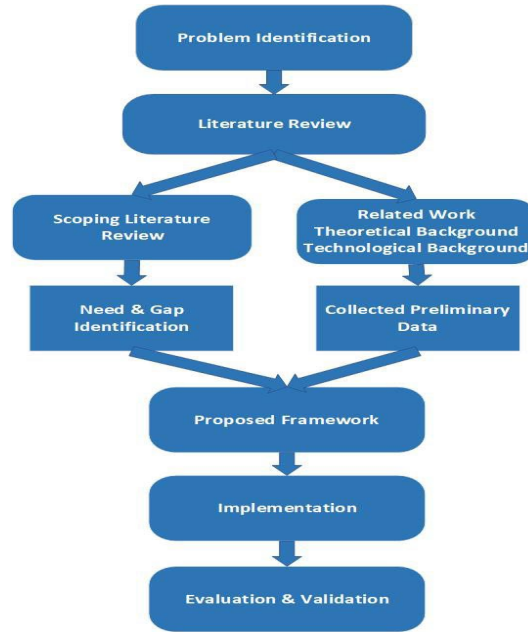


**Figure 1: The Science and Engineering Methodology for Semantic Framework Development**

## 2.1 Research Phases

This research is structured into two main phases, employing scientific and engineering methodologies. The first phase, problem formulation, clearly outlines the definition and origin of the problem. The second phase, proposing a solution, describes in detail the workflow of activities designed to resolve the problem.

### 2.1.1 Problem formalization

The research began with the identification of research problems, followed by a literature review (Buglio et al., 2024b) to explore the different techniques employed to tackle these issues. Based on the existing literature concerning modelling, processing and visualization challenges and verification and validation of IoMT security, the problem is formalized and presented in an algorithmic manner. This algorithm is designed to validate a use case and systematically detect vulnerabilities in Medical IoT devices, identify potential attacks that could exploit these vulnerabilities, assess possible adverse side effects arising from such attacks, and determine appropriate countermeasures to mitigate associated risks. In addition, the algorithm incorporates a governance-mapping layer that classifies detected vulnerabilities into operational, safety, and privacy risk categories, maps them to relevant regulatory controls (e.g., NIST Cybersecurity Framework and ISO/IEC 27001), and generates ontology-based compliance traceability links. This integrated approach ensures that vulnerability detection not only supports technical remediation but also aligns with institutional cybersecurity governance and regulatory requirements.

**Use Case:** If a patient is using a medical device, such as a defibrillator or a blood pressure monitor, which connects to services through network technologies like Wi-Fi or cloud-based systems, there is an inherent risk of vulnerability. These vulnerabilities could potentially be exploited by cyber attackers to compromise device functionality or patient data privacy. This not only jeopardizes patient health but also undermines trust in healthcare technologies. To safeguard both the patient and the device from adverse outcomes, it is crucial to implement robust countermeasures that effectively mitigate these vulnerabilities.

### Algorithm 1 Governance-Aware Vulnerability Detection in Medical IoT Devices

Input: Person  $P$ , Medical Device  $MD$ , Service  $S$ .

Output: Vulnerabilities  $V$ , Attacks  $A$ , Adverse Side Effects  $ASE$ , Countermeasures  $C$ , Risk Categories  $RC$ , Regulatory Controls  $REG$ , Compliance Traceability  $CT$ .

Initialize:

$V \leftarrow \emptyset$

$A \leftarrow \emptyset$

$ASE \leftarrow \emptyset$

$C \leftarrow \emptyset$

$RC \leftarrow \emptyset$

$REG \leftarrow \emptyset$

$CT \leftarrow \emptyset$

**Step 1: Vulnerability Identification**

For each component in Medical Device MD:

Detect vulnerabilities

If vulnerability  $v$  is identified:

Add  $v$  to  $V$

**Step 2: Governance-Aware Risk Classification and Compliance Mapping**

For each vulnerability  $v$  in  $V$ :

$rc \leftarrow \text{ClassifyRiskCategory}(v)$  // Operational, Safety, Privacy

$reg \leftarrow \text{MapToRegulatoryControl}(v)$  // NIST, ISO/IEC 27001, etc.

$ct \leftarrow \text{GenerateComplianceTrace}(v, rc, reg)$

Add  $rc$  to  $RC$

Add  $reg$  to  $REG$

Add  $ct$  to  $CT$

**Step 3: Attack Identification**

For each vulnerability  $v$  in  $V$ :

Identify potential attacks exploiting  $v$

Add identified attacks to  $A$

**Step 4: Adverse Impact Assessment**

For each attack  $a$  in  $A$ :

$ase \leftarrow \text{AssessAdverseSideEffects}(a)$

Add  $ase$  to  $ASE$

**Step 5: Countermeasure Selection**

For each vulnerability  $v$  in  $V$ :

$c \leftarrow \text{SelectCountermeasures}(v)$

Add  $c$  to  $C$

Return:

$V, A, ASE, C, RC, REG, CT$

The structure of *Algorithm 1* directly reflects the gaps identified in the literature and aligns each processing stage with specific security requirements. The vulnerability identification stage captures device-level weaknesses as the foundational input for subsequent analysis. This is followed by attack identification, which addresses a key limitation in existing approaches that often treat vulnerabilities in isolation without explicitly linking them to

potential exploit scenarios. The adverse impact assessment stage extends traditional cybersecurity analysis by incorporating cyber-physical consequences, which is particularly critical in healthcare environments where attacks may directly affect patient safety. Subsequently, the countermeasure selection stage provides actionable mitigation strategies, supporting practical implementation of security controls.

The governance-aware layer, introduced in Step 2, represents the core contribution and primary novelty of this research. This layer integrates structured risk categorization into operational, safety, and privacy domains, maps identified vulnerabilities to relevant regulatory controls and generates ontology-based compliance traceability. Through this integration, vulnerability detection is elevated beyond purely technical remediation to also support compliance reporting, audit readiness, and strategic cyber risk management.

*Algorithm 1* is not intended as a standalone procedure; rather, it is embedded within the proposed semantic framework. Each stage of the algorithm is operationalized through ontology concepts and relationships defined in RDF/OWL, rule-based reasoning mechanisms, and knowledge graph queries over integrated cyber threat intelligence data. This tight integration enables automated, explainable, and scalable vulnerability analysis across complex IoMT environments, supporting both operational security functions and higher-level governance objectives.

### *2.1.2 Proposed solution*

In this research, the primary aim is to develop a governance-aware semantic framework to enhance the security posture of IoT networks used in remote patient monitoring (RPM) systems through partial automation, knowledge integration, and explainable reasoning. The framework leverages domain ontologies, rule-based inference, and knowledge graph technologies to systematically detect vulnerabilities, analyse their impact, and support mitigation planning.

At its core, the framework integrates heterogeneous security knowledge, including device characteristics, vulnerabilities, cyber threat intelligence, and regulatory requirements. Through semantic modelling and reasoning, the framework enables the identification of both known and emerging vulnerabilities, assesses their severity and potential impact, and recommends appropriate countermeasures.

A key distinction of this work is the integration of governance-aware reasoning, where detected vulnerabilities are not only analysed technically but also mapped to risk categories and regulatory controls. This enables traceability between operational security events and institutional compliance requirements, supporting both technical and strategic decision-making.

The solution methodology is structured into four phases, as summarized in Table 1. These phases follow a science and engineering approach, progressing from conceptual design to implementation and validation.

### *2.1.3 Phase I- conceptual model*

In the field of software engineering, conceptualization plays a crucial role. This involves defining principles and design criteria essential for developing the domain ontology. Conceptualization organizes domain knowledge (background knowledge) into a conceptual model that articulates the problem and its solution using domain-specific vocabulary. Such structuring of information simplifies the understanding and communication of complex concepts within the domain.

This model establishes connections between concepts through various properties (relationships) that serve diverse purposes within the Internet of Medical Things (IoMT) context, addressing different scenarios and use cases. It offers a centralized repository and tools that enable effective sharing and communication among all system participants. This not only accelerates the development process but also enhances interoperability and the correlation of test results. This phase has been developed and validated in our previous work (Buglio et al., 2024a) and is reused in this study as the foundational layer for subsequent semantic modelling and reasoning.

Table 1: Solution Methodology Phases

| Solution Methodology Phases |                                     |                                                                                                                                |
|-----------------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Phase                       | Title                               | Description                                                                                                                    |
| Phase I                     | Conceptual Model                    | To define key concepts, relationships, individuals, and axioms for the conceptual model                                        |
| Phase II                    | Prototype Development               | Use semantic web technologies (OWL, RDF, and XML), de facto standards to verify the conceptual model by developing a prototype |
| Phase III                   | Governance-Aware Semantic Framework | To implement the semantic model and store CTI information in a knowledge graph                                                 |
| Phase IV                    | Evaluation and Validation           | Evaluation and validation based on use cases and existing framework                                                            |

#### 2.1.4 Phase II- prototype development

In this phase, a prototype is developed to demonstrate the detailed workings of the proposed conceptual model. It is specifically designed to model and reason about anomalies and vulnerabilities within the IoMT system. The well-defined formalism RDF is utilized to create a domain ontology, capturing the semantics of the domain in terms of concepts and relationships. This includes defining instances of medical devices, vulnerabilities, and IoT networks. Semantic annotation is performed to enrich the domain ontology within the defined setting. This phase builds upon earlier work (Bughio, 2023) and is extended in this study to support integration with governance-aware reasoning mechanisms.

#### 2.1.5 Phase III- governance-aware semantic framework

This phase represents the core contribution of this research. The proposed semantic framework extends prior work by integrating:

- the governance-aware vulnerability detection algorithm (Section 2.1.1),
- regulatory control mapping (e.g., NIST CSF, ISO/IEC 27001), and
- ontology-based compliance traceability.

The framework constructs a semantic model enriched with cyber threat intelligence, including data from the National Vulnerability Database (NVD) via API integration. Rule-based reasoning is applied over the knowledge graph to identify vulnerabilities, infer attack scenarios, assess impacts, and recommend mitigation strategies.

Unlike prior work (Bughio et al., 2024c), which introduced initial semantic modelling, this phase introduces governance-aware reasoning as a novel extension, enabling the alignment of technical vulnerability detection with cybersecurity governance and compliance requirements. This transforms the framework from a technical analysis tool into a decision-support system for both operational and strategic cybersecurity management.

#### 2.1.6 Evaluation and validation

Evaluation and validation are critical for ensuring the reliability and applicability of the proposed framework. The evaluation assesses the effectiveness of vulnerability detection, reasoning accuracy, and governance mapping, while validation confirms alignment with real-world requirements and standards.

In this study, evaluation is conducted across multiple phases. The conceptual model has been evaluated in prior work (Bughio et al., 2024a, 2024c). The prototype implementation has been validated in (Bughio, 2023). The governance-aware semantic framework is evaluated using representative IoMT use cases and knowledge engineering methodologies. These evaluation approaches assess the correctness of reasoning processes, the effectiveness of rule execution, and the overall performance of the framework in identifying vulnerabilities and supporting decision-making.

## 2.2 Strategic and Governance Implications

### 2.2.1 *IoMT as Critical Healthcare Infrastructure*

Healthcare systems are increasingly recognised as part of critical national infrastructure due to their essential role in maintaining public health and societal stability. The digital transformation of healthcare, particularly through IoMT-enabled remote patient monitoring, has introduced unprecedented connectivity and operational efficiency. However, this transformation simultaneously amplifies systemic cyber risk. As noted by the World Health Organization (World Health Organization (WHO), 2021) in its Global Strategy on Digital Health, the expansion of digital health technologies necessitates robust cybersecurity governance to ensure resilience and patient safety.

Cyber incidents in IoMT environments may lead not only to data breaches but also to direct cyber-physical consequences affecting clinical outcomes. Such risks elevate IoMT cybersecurity from a purely technical concern to a strategic issue impacting national resilience, public trust, and institutional accountability. Therefore, vulnerability detection mechanisms must support strategic visibility across device ecosystems rather than operating solely as isolated technical tools.

### 2.2.2 *Alignment with cybersecurity governance frameworks*

Effective cybersecurity in healthcare requires alignment with established governance and regulatory standards. The proposed semantic framework enhances this alignment by mapping detected vulnerabilities to recognised cybersecurity controls, including:

- The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) (The NIST Cybersecurity Framework (CSF) 2.0, 2024), particularly functions related to Identify, Protect, Detect, and Respond.
- The ISO/IEC 27001 standard (International Organization for Standardization, 2022), specifically Annex A.12 addressing operational security controls.
- Guidance provided by the European Union Agency for Cybersecurity (ENISA) (Theocharidou & Lella, 2023) on cybersecurity in the healthcare sector.

By embedding regulatory control mappings within the ontology, the framework enables traceability between technical vulnerabilities and governance obligations, facilitating structured compliance reporting and strategic cyber risk oversight. This supports compliance reporting, audit preparation, and policy-driven security enforcement. Instead of treating compliance as a separate administrative process, the semantic model integrates it directly into the vulnerability detection lifecycle.

### 2.2.3 *Governance-aware risk classification*

The enhanced algorithm introduces governance-aware risk categorisation, classifying vulnerabilities into operational, safety, and privacy risk domains. This classification facilitates structured risk communication across technical, managerial, and executive stakeholders (Kianpour et al., 2022). For example:

- Operational risks affect system availability and service continuity.
- Safety risks impact patient health and device functionality.
- Privacy risks involve unauthorised disclosure of sensitive health information.

By formalising these relationships within the ontology, the framework supports board-level risk dashboards and strategic resource allocation decisions. This transforms vulnerability detection from a reactive technical process into a proactive governance-support mechanism.

### 2.2.4 *Strategic value of semantic automation*

In complex IoMT ecosystems, decision-makers require transparent and accountable security insights to support informed strategic and operational decisions. The integration of knowledge graphs and rule-based reasoning enables traceable inference pathways, allowing security analysts and governance stakeholders to understand how specific vulnerabilities are prioritized and how they relate to regulatory controls. By formalizing relationships between devices, vulnerabilities, risks, and compliance requirements within an ontology-driven structure, the framework enhances visibility, consistency, and accountability in cybersecurity decision-making (Ullah et al., 2025). From a strategic perspective, semantic automation functions as a force multiplier in resource-constrained healthcare environments. It enhances situational awareness, improves consistency in vulnerability assessment, reduces manual analysis overhead, and strengthens cyber resilience across distributed IoMT

infrastructures. Consequently, the proposed framework contributes not only to operational cybersecurity but also to institutional governance maturity and strategic cyber defence capability.

The integration of governance-aware risk classification, regulatory control mapping, and ontology-based compliance traceability demonstrates that semantic automation can extend beyond technical vulnerability detection. By embedding strategic oversight mechanisms directly within the reasoning pipeline, the proposed framework connects operational security processes with institutional governance objectives. This integration provides the foundation for transitioning from isolated vulnerability management toward a structured, resilient, and policy-aligned cybersecurity posture in IoMT-enabled healthcare systems.

### 3. Conclusion

This research presented a knowledge-driven, AI-assisted semantic framework designed to enhance vulnerability detection and cyber resilience in IoMT-enabled remote patient monitoring systems. By integrating domain ontologies, rule-based reasoning, knowledge graph representation, and external cyber threat intelligence, the proposed methodology enables structured, automated, and explainable identification of vulnerabilities, potential attack vectors, adverse cyber-physical impacts, and corresponding countermeasures. The framework advances IoMT cybersecurity by combining technical detection, explainable reasoning, regulatory alignment, and strategic risk management within a unified semantic pipeline, providing a scalable and extensible foundation for cyber defence in complex, heterogeneous healthcare environments. A semantic framework in healthcare is a crucial element in the reduction of cyber warfare exploitation for geopolitical and adversarial operations.

Grounded in a science and engineering research methodology, the framework progresses from conceptual modelling to prototype implementation, semantic integration, and validation against representative use cases. The incorporation of governance-aware risk categorisation and regulatory control mapping extends the contribution beyond purely technical automation, enabling compliance traceability and strategic risk visibility aligned with established cybersecurity frameworks. Evaluation results demonstrate improved consistency, transparency, and timeliness in vulnerability assessment compared to conventional manual approaches. By bridging semantic automation with cybersecurity governance, this work strengthens the resilience of healthcare systems increasingly recognised as critical national infrastructure, and increasingly targeted by hybrid actors.

**Ethics Declaration:** This study is based on conceptual modelling, simulated environments, and representative case scenarios. No real patient data, human participants, or identifiable information were used. Accordingly, formal ethical approval was not required.

**AI Declaration:** No artificial intelligence tools were used in the research methodology preparation, figures, tables or analysis of this manuscript.

### References

- Alam Efat, M. I. et al. (2025). Optimized Energy Consumption in Healthcare WSNs Using Enhanced LEACH Protocol with K-Means. In: Satu, M.S., Shamsul Arefin, M., Lio', P., Kaiser, M.S. (Eds) Proceeding of the 2nd International Conference on Machine Intelligence and Emerging Technologies. MIET 2024. Lecture Notes in Networks and Systems, Vol 1235., 329. [https://doi.org/10.1007/978-981-96-2721-9\\_21](https://doi.org/10.1007/978-981-96-2721-9_21).
- Alsabah, M., et al. (2025). A comprehensive review on key technologies toward smart healthcare systems based IoT: technical aspects, challenges and future directions. Artificial Intelligence Review, 58(11). <https://doi.org/10.1007/s10462-025-11342-3>.
- Basili, V. R. (1993). The experimental paradigm in software engineering (pp. 1–12). [https://doi.org/10.1007/3-540-57092-6\\_91](https://doi.org/10.1007/3-540-57092-6_91).
- Bughio, K. S. (2023). Knowledge Organization System for Partial Automation to Improve the Security Posture of IoMT Networks. Procedia Computer Science, 3471–3478. <https://doi.org/10.1016/j.procs.2023.10.342>.
- Bughio, K. S., Cook, D., & Shah, A. A. (2024a). Developing a Novel Ontology for Cybersecurity in Internet of Medical Things-Enabled Remote Patient Monitoring. Sensors, 24(9), 2804. <https://doi.org/10.3390/s24092804>.
- Bughio, K. S., Cook, D., & Shah, A. A. (2024b). Investigating the intersections of vulnerability detection and Internet of Medical Things (IoMT) in healthcare, a scoping review protocol for Remote Patient Monitoring. Research, Society and Development, 13(6), e11313646080. <https://doi.org/10.33448/rsd-v13i6.46080>.
- Bughio, K. S., Cook, D., & Shah, A. A. (2024c). Novel Knowledge Graph-Based Modeling for Vulnerability Detection in the Internet of Medical Things (pp. 314–325). [https://doi.org/10.1007/978-981-97-5937-8\\_26](https://doi.org/10.1007/978-981-97-5937-8_26).
- Deb, S. et al. (2025). Securing the Internet of Medical Things (IoMT): Real-World Attack Taxonomy and Practical Security Measures. ArXiv. <https://doi.org/10.48550/arXiv.2507.19609>.
- Ewoh, P., & Vartiainen, T. (2024). Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. In Journal of Medical Internet Research (Vol. 26, p. e46904). JMIR Publications Inc. <https://doi.org/10.2196/46904>.

- Hansel, M., & Silomon, J. (2024). Ransomware as a threat to peace and security: understanding and avoiding political worst-case scenarios. *Journal of Cyber Policy*, 9(2), 159–178. <https://doi.org/10.1080/23738871.2024.2357092>.
- International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection- Information security management systems-Requirements (Third Edition 2022). ISO/IEC 27001:2022 –10. <https://www.exactls.com/wp-content/uploads/2025/02/ISO-IEC-270012022-ed.3.pdf>.
- Kapsokoli, E. (2025). Weaponizing Cyberspace: The Russia-Ukrainian War. *Security Science Journal*, 6(2), 71–97. <https://doi.org/10.37458/ssj.6.2.3>.
- Kelly, A. E. et al. (2008). *Handbook of Design Research Methods in Education*.; 1st Edition. Routledge. <https://doi.org/10.4324/9781315759593>.
- Kianpour, M., Kowalski, S. J., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, 116. <https://doi.org/10.1016/j.simpat.2022.102493>.
- Ojha, A., & Gupta, B. (2025). Evolving landscape of wireless sensor networks: a survey of trends, timelines, and future perspectives. In *Discover Applied Sciences* (Vol. 7, Number 8). Springer Nature. <https://doi.org/10.1007/s42452-025-07070-6>.
- Pritika, P., Shanmugam, B., & Azam, S. (2023). Risk Assessment of Heterogeneous IoMT Devices: A Review. *Technologies*, 11(1), 31. <https://doi.org/10.3390/technologies11010031>.
- Shah, T. et al. (2026). A systematic review of emerging trends of IoT in healthcare and IoMT frameworks. *Discover Public Health*, 23(1). <https://doi.org/10.1186/s12982-026-01347-w>.
- Sripriyanka, G., & Mahendran, A. (2021). A study on security privacy issues and solutions in internet of medical things—A review. In *Intelligent IoT Systems in Personalized Health Care* (pp. 147–175). Elsevier. <https://doi.org/10.1016/B978-0-12-821187-8.00006-X>.
- The NIST Cybersecurity Framework (CSF) 2.0. (2024). <https://doi.org/10.6028/NIST.CSWP.29>.
- Theocharidou, M., & Lella, I. (2023). ENISA Threat Landscape Report: Health Sector (January 2021 to March 2023). European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf>.
- Ullah, U., Haleem, M., & Ullah, A. (2025). OntoSecAI: Ontology-driven security automation for AI-enabled systems. *PLOS One*, 20(12), e0337806. <https://doi.org/10.1371/journal.pone.0337806>.
- World Health Organization (WHO). (2021). *Global Strategy on Digital Health 2020-2025*. [online] <https://iris.who.int/server/api/core/bitstreams/1f4d4a08-b20d-4c36-9148-a59429ac3477/content>