Enhancing Risk Management on IoT Medical Devices

Ilkka Tikanmäki[1 2], Jyri Rajamäki[1], Tomas Liettyä[1], Sara Lindholm[1], Nina Steiner[1] and Timo Tolonen[1]

[1]Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland
[2]Department of Warfare, National Defence University, Helsinki, Finland

ilkka.tikanmaki@laurea.fi
jyri.rajamaki@laurea.fi
tomas.liettya@student.laurea.fi
sara.lindholm@student.laurea.fi
nina.steiner@student.laurea.fi
timo.tolonen@student.laurea.fi

Abstract: The Internet of Medical Things (IoMT) represents a transformative step in healthcare, enhancing patient outcomes through real-time monitoring and treatment. However, the increasing reliance on IoMT devices exposes critical vulnerabilities, posing significant risks to patient safety and healthcare operations. This paper evaluates the cybersecurity challenges of IoMT devices and explores how the DYNAMO tools (Cyber-Attack Forecasting, Secure AI, ThreatLens, and CTI Extractor) address these threats. A phased research approach was employed, with a literature review, DYNAMO tool analysis, and vulnerability-tool mapping. The results demonstrate the potential of advanced AI-driven tools to predict, detect, and mitigate threats, ensuring robust security for IoMT ecosystems. The research found promising results but acknowledges limitations due to the theoretical nature of the analysis. Without practical testing, the feasibility of these tools in real-world IoMT environments remains uncertain. For instance, CAF and CTI Extractor rely heavily on accurate and comprehensive data, which may not always be available in healthcare organisations. Secure AI's computational demands and ThreatLens's complex visualisations may present barriers, particularly for smaller healthcare facilities with limited resources or expertise.

Keywords: Internet of Medical Things, Cybersecurity, Medical device security, Cyber threats, DYNAMO tools

1. Introduction

1.1 Background and Research Problem

The healthcare sector is increasingly adopting Internet of Medical Things (IoMT) devices, integrating smart technologies to enhance medical care. These devices connect patients, healthcare providers, and systems, enabling real-time data exchange (Li, Wang, J., Wang, S. & Zhang 2023). However, the interconnected nature of IoMT introduces vulnerabilities that can jeopardise patient safety and system integrity. Cyber threats such as denial-of-service (DoS) attacks, data breaches, and remote manipulation highlight the urgent need for effective risk management strategies. (Puat & Rahman 2020; Smith, 2020)

The DYNAMO project (2023) aims to enhance cybersecurity and resilience in three critical sectors, one of which is healthcare. DYNAMO develops and utilises advanced tools that help predict, detect, and mitigate cyber threats in healthcare environments.

1.2 Objectives and Research Questions

This study focuses on the capabilities of DYNAMO cybersecurity tools, such as Cyber-Attack Forecasting, Secure AI, ThreatLens, and CTI Extractor to mitigate risks associated with IoMT devices. The paper aims to provide actionable insights into leveraging these tools to improve IoMT security while addressing their limitations.

This study seeks to answer the following questions:

- What are the key cybersecurity challenges of IoMT devices?
- How can DYNAMO tools, such as Cyber-Attack Forecasting, Secure AI, ThreatLens, and CTI Extractor, help manage these challenges?
- What are the limitations and challenges of DYNAMO tools in practical applications within healthcare environments?

1.3 Structure of the Report

Following this introduction, Section 2 outlines the research methods and approach used in this study. Section 3 presents the results of the literature review. Section 4 details the tool analysis and its findings. Section 5,

"Mapping Analysis," integrates the identified vulnerabilities with the analysed tools. Finally, Section 6 concludes the article, presenting the conclusions and suggesting areas for future research.

2. Research Methodology and Approach

2.1 Three-Phase Research Model

A three-phase research approach was undertaken. This research methodology can be described as a multi-phase approach that combines a literature review, tool analysis, and vulnerability-to-tool mapping analysis. This approach typically falls within the design science research (DSR) (Hevner et al. 2004; Peffers, et al. 2007; Vaishnavi & Kuechler, 2007) framework, aiming to understand, analyse, and develop solutions to a specific problem. The progression is structured in phases, each with a clear role in data collection, analysis, and evaluation. Phase one involved a literature review that identified vulnerabilities in IoMT devices, including weaknesses in wireless connections and risks of external access. In the second phase, DYNAMO tools were analysed to assess their functionality and relevance to IoMT security. The third phase involved mapping vulnerabilities to the capabilities of DYNAMO tools to evaluate their effectiveness in real-world scenarios. Table 1 describes how the applied research approach relates to scientific methodologies.

Table 1: Research approach and applied scientific methods.

Phase	Method Type	Purpose
Phase 1: Literature Review	*Literature Review:* This phase is based on a systematic approach, analysing existing research focusing on IoMT device vulnerabilities.	To identify the theoretical background and map the problem area.
Phase 2: Tool Analysis	*Empirical Analysis:* In this phase, specific tools (DYNAMO tools) are analysed to evaluate their functionality and relevance from an IoMT security perspective.	To assess and compare technological solutions in the context of identified vulnerabilities.
Phase 3: Vulnerability-to-Tool Mapping	*Practical Evaluation and Testing:* This phase combines the vulnerabilities identified in the literature review with the results of the tool analysis, evaluating the effectiveness of the tools in real-world scenarios.	To provide practical solutions and recommendations for mitigating vulnerabilities.

The applied research approach combines deductive and inductive reasoning:

- Deductive: Concepts and vulnerabilities identified in the literature review guide the subsequent phases.
- Inductive: The results of the analysis and mapping generate new insights into the effectiveness and applicability of the tools.

The applied research methodology resembles the design science research process but can also be classified as exploratory research, as it seeks to map out new solutions for improving the security of IoMT devices.

3. Literature Review

The literature review examines factors affecting risk management in IoMT that relate to medical devices. The review assesses the cyber security challenges of IoMT devices and examines the use of DYNAMO tools (in Chapter 4). The literature review focused on the vulnerabilities in IoMT devices, the functionality of DYNAMO tools, and whether they are suitable for IoMT. Multiple sources of information were used to validate the results, ensuring a triangular measurement of data. Understanding the current state of healthcare equipment was ensured by this approach. The current situation of IoMT equipment research was understood through desktop research on academic magazines, technical reports, conference papers, and journal papers carried out in this study.

3.1 Current State of IoMT Device Security

The Internet of Medical Things (IoMT) represents a significant advancement in the healthcare sector, where medical devices are interconnected and transmit real-time data to improve patient care. IoMT is a combination of medical devices and the Internet of Things (IoT). IoMT systems represent the future of current healthcare systems, where every medical device is connected and monitored via the internet by healthcare

professionals. This development offers faster and more affordable healthcare. Figure 1 illustrates an example of IoMT systems, where a patient's vital signs are collected using sensor devices and transmitted to IoMT applications via the internet. The information then flows to healthcare experts and medical staff, after which a response is sent back to the necessary patients. (Razdan & Sharma 2022)

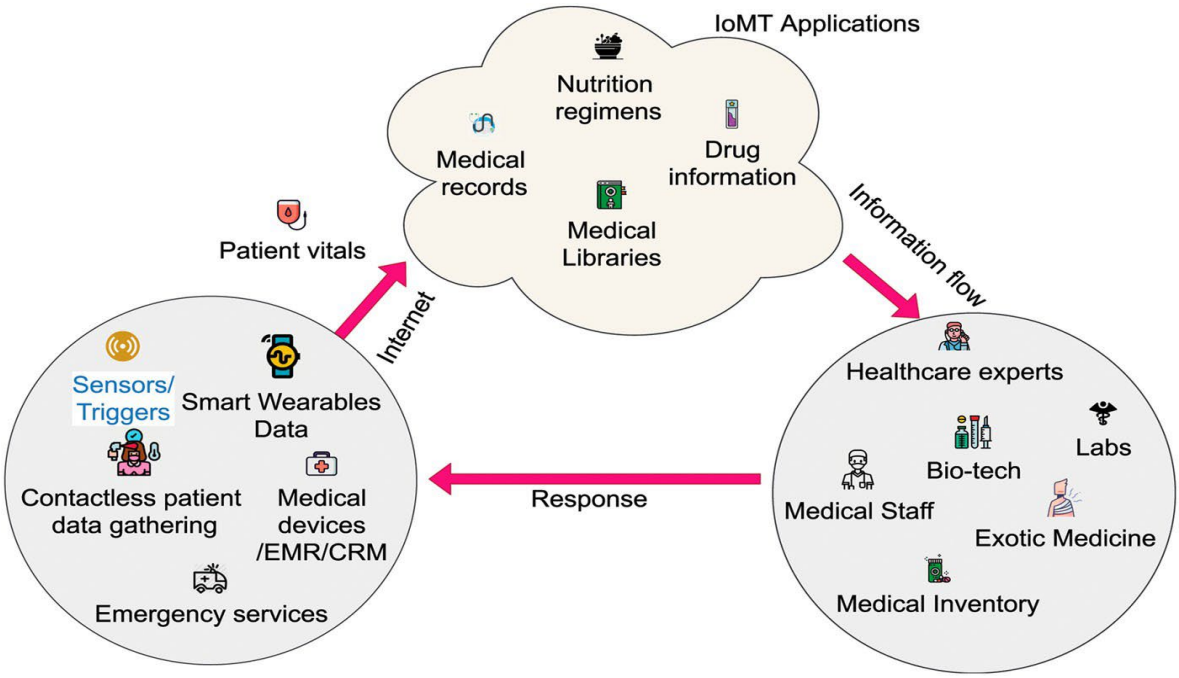

Figure 1: Principle on Internet of Medical Things (Razdan & Sharma 2022)

This vision of the future is already a reality. One of the primary applications of IoMT is wearable devices. From smartwatches that measure heart rate to patches that monitor vital signs, these devices are no longer just for fitness enthusiasts. They are becoming essential for managing chronic diseases, remote monitoring, and even predicting health issues, enabling quicker patient care and potentially saving lives (Kamalov et al. 2023).

Another significant application area is smart hospitals. These hospitals leverage IoMT technology to optimise operations and improve patient outcomes. Examples include automated medication dispensers, connected imaging devices, and smart surgical tools. This technology enhances accuracy and reduces human errors, making healthcare more efficient and safer (Ghadi et al. 2024).

Remote patient monitoring is another revolutionary development. With IoMT, doctors can monitor patients without requiring them to visit the hospital. Devices such as glucose meters, blood pressure monitors, and smart clothing transmit data directly to healthcare professionals. This continuous flow of information enables proactive disease management, reduces hospital visits, and improves the quality of life (Hireche, Mansouri & Pathan 2022).

Data privacy and security are of utmost importance. Healthcare professionals must ensure that all IoMT devices comply with strict data protection regulations. Strong encryption, regular updates, and vigilant monitoring are essential to protect patient information (Al Khatib, Shamayleh & Ndiaye 2024).

The Internet of Medical Things is transforming healthcare. By harnessing this technology, we can provide more personalised, efficient, and impactful care. The future of health technology is here, and it is interconnected.

3.2 Identified Vulnerabilities

IoMT devices were found to be highly susceptible to attacks due to weak wireless communication protocols, such as Bluetooth and Wi-Fi, which allow for eavesdropping, spoofing, and other forms of exploitation. External access risks, including the potential manipulation of life-critical devices like pacemakers and insulin pumps, were identified as a significant threat to patient safety (Puat & Rahman 2020; Smith, 2020). Additionally, denial-of-service (DoS) attacks were recognised as a major risk to healthcare operations, potentially delaying critical care and disrupting services (Smith, 2020). Data breaches involving unauthorised access to sensitive patient information further compound these risks, leading to privacy violations, regulatory penalties, and reputational damage (Puat & Rahman 2020; Smith, 2020).

4. Tool Analysis

This chapter presents DYNAMO tools, their functionality and relevancies and an analysis of the tools.

4.1 Overview of DYNAMO Tools

An automated framework called a computer-aided risk analysis tool (CAR) allows users to conduct a computerised risk analysis of their information system. A static diagram that can be analysed rapidly for vulnerabilities, attack paths, hotspots, etc., is created by combining hardware and software layers. The most efficient attack path among the possible ones is identified using a cost-based method. The Data Anonymization Tool (DAT) is a reliable method for ensuring data anonymisation and privacy before sharing and using. The DAT tool is made up of a single web interface and an easily customisable, yet simple, anonymisation engine. A dataset can be configured, and anonymisation models can be chosen. The configuration is carried out in stages to help a non-expert user navigate the anonymisation process.

A secure and flexible approach to sharing information between data providers and consumers is provided by fine-grained access (FGA) control, built on attribute-based encryption (ABE). To ensure controlled access to shared information, the system includes data providers, data consumers, a storage service (data leak), and access authorities. The objective of this framework is to enable secure collaboration among multiple organisations and entities by utilising attribute-based encryption, which provides a distributed, robust, and secure fine-grained access control policy.

The Cyber Attack Prediction Tool (CAF) provides next-minute cyber-attack predictions. The tool also considers the type of cyber-attack (DoS, DDoS, etc.) and takes into account network traffic measurements. Destination ports (DPs) are the tool's primary focus, and only target DP measurements are considered to provide predictions of upcoming cyber-attacks (forecasts for the next minute). Cyber Knowledge Graph (CKG) is a system that manages cyber security intelligence, collecting and coordinating threat intelligence-related information from different sources and mapping it to ontology concepts. Cyber security concepts and related ones are included in ontology, such as IT infrastructure subject to cyber-attacks. The impact of cyber threats can be better understood by security analysts by querying and analysing this information.

The CTI Extractor is responsible for gathering, extracting, analysing, and correlating CTI from external and internal sources. CERT feeds, Proof of Concept (PoC) exploits, social media, forums, and relevant web pages from the Surface Web and Dark Web are some of the external sources that can be found. Companies can assess their resilience to potential natural and man-made disturbances through the support of the Fraunhofer Resilience Evaluator (FReE). Using the FReE tool, companies can measure the resilience of their business unit, facilities, or systems in a meaningful manner. The FReE tool brings together diverse technical, organisational, social, and economic challenges that pertain to the resilience of any business. This provides a comprehensive understanding of their business capabilities and constraints to threats for the experienced user. This lightweight tool is designed well and can help with a detailed assessment of their systems/companies' resilience.

The simulation of single/multi-point failures in a modelled CI can be done using Caesar, a tool built on graphs and agents. Physical, cyber, or cyber-physical events and threats can lead to failures that are either direct or indirect. Offline and online methods can be used to analyse network impacts. The offline analysis involves analysing the network's stochastic properties with single-point and multi-point failures to determine the most ineffective combinations. The online analysis utilises data from an appropriate integrated platform to conduct real-time analysis of specific threats and failures in the network.

Secure AI is a cybersecurity and inspection tool powered by AI that can identify data irregularities, threats, and risks from various data sources. Users are given the knowledge and tools to protect themselves against cyber threats and malicious software, and organisations are assisted in creating and maintaining secure systems. To better protect themselves from cyber-attacks, Secure AI offers training material, interactive simulations, and up-to-date resources.

Public health protection and common interoperability can be enhanced through the significant improvement of the existing knowledge base of S-HELP. Next-generation decision support tools (DS) and a user-centred decision support system (DSS) need to be developed to ensure improved preparedness, rapid response, and coordinated recovery in emergencies. ThreatLens is an interactive platform for security analysts and professionals to learn about potential threats, vulnerabilities, and attacks through security visualisation applications. Visual analytics and Natural Language Processing (NLP) approaches are employed by the

ThreatLens extension application to discover trends, vulnerabilities, and threats and to determine the severity of vulnerabilities. To improve their security posture using third-party datasets, enterprises can use ThreatLens as a Security Information and Event Management (SIEM) system and a complementary security database.

The Early Warning System (EWS) is a platform for sharing information about cyber incidents and cyber defence. The exchange of structured threat and vulnerability information and cross-organizational incident collaboration are the purposes of using it. In a wiki-based manner, unstructured information can also be exchanged by using it. Pianista, an AI-powered design tool, gathers data from a world representation (i.e., domain) and a problem representation. The tool uses design algorithms to create an action plan that solves the problem. Pianista aims to automatically generate solutions to problems by following specific actions to solve them. The tool requires inputs representing the world (as a 'domain'), its current state, and the desired final state. Classical AI design algorithms and heuristics are employed to generate plans.

4.2 Analysis Results

The theoretical analysis of the DYNAMO tools suggested their strong potential to address these vulnerabilities. CAF emerged as a key tool for proactive threat management, leveraging AI to predict cyberattacks by analysing historical data and identifying patterns. Its ability to provide early warnings could help healthcare organisations reduce response times and minimise the impact of incidents. Secure AI was identified as effective for real-time anomaly detection, especially in data-intensive IoMT environments, enabling quick identification and mitigation of threats. ThreatLens demonstrated utility in visualising and prioritising vulnerabilities, allowing security teams to focus on the most critical risks. Lastly, CTI Extractor provided a comprehensive view of emerging threats by integrating internal and external threat intelligence, enhancing situational awareness, and enabling pre-emptive action.

5. Mapping Analysis: Linking Vulnerabilities to Tools

5.1 Mapping Vulnerabilities to Tool Capabilities

The research identified critical cybersecurity vulnerabilities in IoMT devices and explored the theoretical application of DYNAMO tools—Cyber-Attack Forecasting (CAF), Secure AI, ThreatLens, and CTI Extractor—to mitigate these threats.

5.2 Evaluating Tool Effectiveness in Practical Scenarios

5.2.1 Use Case 1: Malware infection via IoMT device

As IoMT devices become critical to healthcare, they also create vulnerabilities, particularly malware attacks. For example, an attacker could exploit outdated software in a wireless infusion pump to deploy malware across the hospital's network. Such infections could lead to data breaches, system downtime, and disruptions in patient care.

The DYNAMO tools mitigate this risk by employing Cyber-Attack Forecasting (CAF) to identify potential attack vectors and Secure AI for real-time anomaly detection. ThreatLens visualises attack pathways, enabling administrators to respond quickly to threats. CTI Extractor gathers and analyses threat intelligence, helping predict and prevent future incidents (DYNAMO-WP2 Use Cases Scenarios - Hospital, 2024).

Malware in healthcare, especially ransomware targeting critical systems, poses severe risks. Smith (2020) highlights that attackers increasingly exploit connected medical devices, necessitating layered defence strategies. The DYNAMO tools' proactive monitoring ensures operational resilience and patient safety.

5.2.2 Use case 2: Denial of Service Through Internal Network Socket

Hospitals face risks from physical access to internal network sockets, which attackers can exploit to launch denial-of-service (DoS) attacks. For instance, an attacker might connect a rogue device to an unsecured network port, disrupting access to systems like Laboratory Information Systems (LIS). Such attacks delay diagnoses and endanger patient care.

The DYNAMO platform provides robust defences. Secure AI detects unauthorised devices and unusual traffic patterns in real-time. CAF predicts attack vectors, and ThreatLens visualises vulnerabilities, allowing rapid response to physical and network-based threats (DYNAMO- WP2 Use Cases Scenarios - Hospital, 2024).

Smith (2020) emphasises the rising frequency of physical access exploits, urging hospitals to strengthen physical and network security. DYNAMO's integrated tools help prevent such scenarios, ensuring uninterrupted care delivery.

5.3 Key Findings and Gaps

The study underscores the critical role of advanced cybersecurity tools in safeguarding IoMT ecosystems. DYNAMO tools demonstrate significant potential in detecting and mitigating threats through AI-driven insights and comprehensive threat intelligence.

6. Discussion and Conclusions

6.1 Summary of results

The findings underline the importance of adopting advanced cybersecurity tools to address the vulnerabilities of IoMT devices. The theoretical evaluation demonstrates that tools like CAF can shift IoMT security from a reactive to a proactive approach by predicting and pre-empting potential threats (DYNAMO, 2023). Secure AI complements this by continuously monitoring IoMT environments for anomalies, ensuring real-time protection (DYNAMO, 2024). ThreatLens adds value by mapping vulnerabilities and prioritising response efforts, while CTI Extractor enhances threat intelligence, enabling organisations to counter known and emerging threats (Rajamäki & McMenamin, 2024).

6.2 Recommendations for Risk Management in IoMT Devices

Based on the analysis of the tools, the following recommendations can be made for IoMT risk management using DYNAMO tools:

1. **Proactive Threat Management:**

- **Cyber-Attack Forecasting (CAF)**: Utilize AI-based tools to predict cyberattacks by analysing historical data and identifying attack patterns. This can help healthcare organisations reduce response times and minimise the impact of incidents.

2. **Real-Time Anomaly Detection:**

- **Secure AI**: Leverage AI-based tools for real-time anomaly detection, especially in data-intensive IoMT environments. This enables quick identification and mitigation of threats.

3. **Visualization and Prioritization of Vulnerabilities:**

- **ThreatLens**: Use tools to visualise and prioritise vulnerabilities, helping security teams focus on the most critical risks.

4. **Integration of Threat Intelligence:**

- **CTI Extractor**: Collect and analyse threat intelligence from internal and external sources. This enhances situational awareness and enables pre-emptive actions against threats.

5. **Training and Resource Optimization:**

- Train healthcare IT teams to effectively use tools like ThreatLens to maximise their impact.
- Optimize tools like Secure AI for resource-constrained environments and develop frameworks to integrate these tools with legacy systems.

6. **Practical Testing and Validation:**

- Validate the tools in real-world settings or high-fidelity simulations to assess their practical applicability and address potential challenges.

6.3 Limitations of the Study

Despite these promising findings, the research acknowledges limitations due to the theoretical nature of the analysis. Without practical testing, the feasibility of these tools in real-world IoMT environments remains uncertain. For instance, CAF and CTI Extractor rely heavily on access to accurate and comprehensive data, which may not always be available in healthcare organisations (DYNAMO, 2023; Rajamäki & Tiitta, 2024). Secure AI's computational demands and ThreatLens's complex visualisations may present barriers to adoption, particularly for smaller healthcare facilities with limited resources or expertise (DYNAMO, 2024).

6.4 Suggestions for Future Research

Further development is necessary to address challenges such as legacy device integration, false positives, and information overload. Future research should focus on enhancing these tools' adaptability and refining their performance in evolving IoMT environments. Future research should focus on validating these tools in real-world settings or high-fidelity simulations to assess their practical applicability and address potential challenges.

Optimising tools like Secure AI for resource-constrained environments and developing frameworks to integrate these tools with legacy systems will be critical to ensuring broader adoption. Training healthcare IT teams to effectively utilise tools such as ThreatLens can further maximise their impact (DYNAMO, 2024; Rajamäki & McMenamin, 2024).

Acknowledgements

This study has received funding from the European Union project DYNAMO, the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 101069601 and The Cybersecurity in Everyday Work in the Social and Healthcare Sector (KyberSoTe) project. The views expressed are those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

References

Al Khatib, I.; Shamayleh, A.; Ndiaye, M. Healthcare and the Internet of Medical Things: Applications, Trends, Key Challenges, and Proposed Resolutions. Informatics 2024, 11, 47. https://doi.org/10.3390/informatics11030047

DYNAMO (2023) Factsheet 2: Cyber Threat Intelligence. Available at: https://horizon-dynamo.eu/wp-content/uploads/2023/09/DYNAMO-Factsheet-2-1.pdf

DYNAMO (2024) Factsheet 5: Cyber Crisis Communication and Enhancement of Organizational Resilience. Available at: https://horizon-dynamo.eu/wp-content/uploads/2024/06/DYNAMO_fact_sheet_05.pdf

Ghadi, Y.Y., Mazhar, T., Shahzad, T. et al. The role of blockchain to secure internet of medical things. Sci Rep 14, 18422 (2024). https://doi.org/10.1038/s41598-024-68529-x

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). "Design Science in Information Systems Research" (MIS Quarterly).

Hireche, R.; Mansouri, H.; Pathan, A.-S.K. Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis. J. Cybersecur. Priv. 2022, 2, 640-661. https://doi.org/10.3390/jcp2030033

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

Li, C., Wang, J., Wang, S. and Zhang, Y. 2023. A Review of IoT Applications in Healthcare. Neu- rocomputing. Accessed 12.10.2024. Available at: https://doi.org/10.1016/j.neucom.2023.127017.

Palo Alto Networks (2024) 'What is IoMT Security?', Palo Alto Networks Cyberpedia. Accessed: 22.11 2024. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-iomt- security.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). "A Design Science Research Methodology for Information Systems Research" (Journal of Management Information Systems).

Puat, H., Rahman, A. 2020. (PDF) IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy. Accessed 12.10.2024. Available at: https://www.researchgate.net/publication/347968462_IoMT_A_Review_of_Pacemaker_Vulnerabilities_and_Security_Strategy.

Rajamäki, J. & McMenamin, S., 2024. Utilization and Sharing of Cyber Threat Intelligence Produced by Open-Source Intelligence. International Conference on Cyber Warfare and Security. https://papers.academic-conferences.org/index.php/iccws/article/view/2069.

Rajamäki, J. & Tiitta, K., 2024. Implementation of OSINT for Improving an International Finance Sector Organization's Cybersecurity. International Conference on Cyber Warfare and Security. https://papers.academic-conferences.org/index.php/iccws/article/view/1977.

Razdan S. & Sharma, S. 2022. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies, IETE Technical Review, 39:4, 775-788, DOI: 10.1080/02564602.2021.1927863

Smith, E. 2020. Hacking Humans: A Glimpse into the Future of Hacking Wireless Medical Devices. ResearchGate. Accessed 12.10.2024. Available at: https://doi.org/10.13140/RG.2.2.11973.27367.