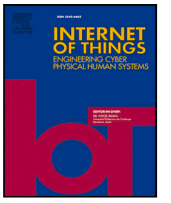
Internet of Things 29 (2025) 101437

Contents lists available at ScienceDirect

Internet of Things

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



Dynamic risk assessment approach for analysing cyber security events in medical IoT networks

Ricardo M. Czekster [a,*], Thais Webber [a], Leonardo Bertolin Furstenau [b], César Marcon [c]

[a] Aston University, School of Computer Science & Digital Technologies, Aston Street, Birmingham, B4 7ET, UK
[b] UFRGS, Federal University of Rio Grande do Sul, Graduate Program in Industrial Engineering, Porto Alegre, 90035-190, Brazil
[c] PUCRS University, Graduate Program in Computer Science (PPGCC), Av. Ipiranga, 6681, Porto Alegre, 90619-900, RS, Brazil

ARTICLE INFO

Keywords:
Medical Internet of Things (MIoT)
Cyber security
Dynamic risk assessment
Simulation models
Data integration
Threat analysis

ABSTRACT

Advancements in Medical Internet of Things (MIoT) technology ease remote health monitoring and effective management of medical devices. However, these developments also expose systems to novel cyber security risks as sophisticated threat actors exploit infrastructure vulnerabilities to access sensitive data or deploy malicious software, threatening patient safety, device reliability, and trust. This paper introduces a lightweight dynamic risk assessment approach using scenario-based simulations to analyse cyber security events in MIoT infrastructures and supplement cyber security activities within organisations. The approach includes synthetic data and threat models to enrich discrete-event simulations, offering a comprehensive understanding of emerging threats and their potential impact on healthcare settings. Our simulation scenario illustrates the model's behaviour in processing data flows and capturing the characteristics of healthcare settings. Our findings demonstrate its validity by highlighting potential threats and mitigation strategies. The insights from these simulations highlight the model's flexibility, enabling adaptation to various healthcare settings and supporting continuous risk assessment to enhance MIoT system security and resilience.

1. Introduction

Trends in digital healthcare emphasise maintaining a continuous connection between patients and hospitals while safeguarding confidentiality and ensuring privacy [1]. This can be achieved by effectively integrating technologies such as the Medical Internet of Things (MIoT), cloud computing, virtual reality, virtual machines, and low-power wireless networks [2]. Among these, MIoT is a vital base technology, forming a network for interconnecting devices and sensors specifically designed for healthcare applications [3]. These devices collect, transmit, and analyse medical data in real-time, facilitating patient monitoring and medical equipment management [1]. Examples of MIoT devices are blood pressure monitors and smartwatches, which are prevalent in hospitals and widely accessible to the healthcare community, allowing bi-directional communication of patients, staff and equipment [2]. Substantial work is concerned with integrating multiple IoT in healthcare using various technologies and allowing automatic data analysis [4,5].

Although MIoT in healthcare offers significant benefits, it also exposes the digital space to threat actors and malicious activities [6–10]. It has been reported that the issue of *excessive alerting* [11] is a significant problem in Information and Communication Technologies (ICT) systems and sub-systems within complex solutions across various domains (not limited to healthcare). This problem is further compounded when security tools are integrated into the analysis, as they often produce numerous false positives

* Corresponding author.
E-mail address: r.meloczekster@aston.ac.uk (R.M. Czekster).

https://doi.org/10.1016/j.iot.2024.101437
Received 29 June 2024; Received in revised form 1 October 2024; Accepted 13 November 2024
Available online 20 November 2024

and duplicated alerts, requiring extensive investigation and overwhelming response teams. AI-assisted approaches [12,13] have been proposed to address this problem, along with optimised inspections of Security Operations Centre (SOC) critical paths [14]. The organisation sometimes does not understand cyber security requirements clearly, causing researchers to formalise them over technical and quantitative aspects [15].

Numerous surveys and systematic literature reviews have demonstrated the research community's interest in MIoT cyber security [16–19]. Generally, research topics involve potential paths for adversarial attacks [20,21], specific IoT attacks [19] and infrastructure-supporting systems [22]. However, these prior studies had limitations, such as not providing explicit guidance on dynamic strategies for anticipating and responding to cyber-attacks or exploring in-depth how different technologies could support the cyber security of MIoT. Recent research emphasises the need for an integrated approach, combining multiple digital technologies and solutions to support healthcare cyber–physical resilience [23].

In this work, we propose the use of simulation to better understand data flows in interconnected hospital systems, helping teams prioritise and address critical cyber security events, particularly in resource-limited environments where the volume of alerts and attack complexity can overwhelm resources [24]. Simulation, recently combined with Digital Twins (DT) concepts [25], enhances the ability to anticipate, monitor, and respond to cyber-attacks by providing a structured framework for efficient interventions [25,26]. While MIoT systems can incorporate redundancy and automated alerts to ensure secure operations, these features are often lacking due to poor design or requirement elicitation [27]. This research integrates Discrete-event Simulation (DES) and threat modelling to analyse the potential misuse of MIoT infrastructures.

Our approach applies dynamic risk assessment through scenario-based simulations to identify and mitigate emerging cyber security threats, leveraging real-time infrastructure data for proactive defence. These simulations, driven by synthetic data, represent the MIoT system and simulate cyber security events based on threat models. For real-world MIoT applications, this framework can be instantiated with actual infrastructure data while maintaining generalisation. Combined with threat models that capture cyber threat events, this approach remains adaptable across various system configurations. While simulations provide valuable insights, they also introduce significant computational overhead and increase energy consumption - critical limitations in resource-constrained MIoT environments [28]. Given these constraints, the following research question arises: *'How to employ simulation-based technology to anticipate, monitor and respond to a wider range of cyber-attacks in diverse, real-world MIoT settings without compromising system performance or resource efficiency?'*.

We address this question through the following structure. Section 2 outlines the cyber security context in MIoT and the benefits of a dynamic risk assessment approach. Section 3 details the conceptual approach, presenting a simulation model applied to a synthetic smart hospital case study. Finally, Section 4 summarises the contributions, discusses potential extensions and implications, and concludes with considerations on the persistent and evolving threats in MIoT networks and practices to mitigate cyber risks.

2. Research background in MIoT cyber security

MIoT integrates IoT technologies into healthcare, providing significant benefits such as remote monitoring and efficient data collection [29,30]. However, with these advancements come considerable cyber security challenges. Over the years, MIoT cyber security has evolved to address these shortcomings, focusing on Confidentiality, Integrity, and Availability (CIA) [31]. For instance, Tarish et al. (2024) [32] integrated machine learning and blockchain to enhance network security in MIoT, specifically targeting the challenges of maintaining CIA in these evolving networks.

Early MIoT systems employed traditional encryption techniques to secure data transmission and storage, but these methods were often insufficient due to the unique constraints of MIoT devices, such as limited computational power and energy resources [29]. As the volume of medical data and the complexity of cyber threats increase, the need for specialised cryptographic solutions tailored to MIoT's specific requirements becomes evident [30]. Researchers have proposed innovative approaches to meet these requirements, such as trust-based frameworks and more machine learning-enhanced intrusion detection systems [1,30]. These advanced techniques provide real-time threat detection and response, ensuring sensitive medical data remains protected from unauthorised access and cyber-attacks [8,31]. In addition, developing lightweight authentication and key agreement schemes is crucial for maintaining secure communications within MIoT environments without overburdening the devices [31]. Meanwhile, the hybrid encryption model discussed by Jyotheeswari and Jeyanthi (2020) [29], which integrates symmetric and attribute-based encryption, highlights the importance of securely managing large volumes of medical data and demonstrates the need for specialised cryptographic solutions tailored to the unique demands of MIoT.

Despite these advancements, significant challenges remain in MIoT cyber security, particularly in maintaining data integrity and confidentiality while managing the limited computational capabilities of MIoT devices. Addressing this requires developing lightweight algorithms and optimising security protocols for low-power devices, ensuring robust yet efficient data protection without overburdening the devices [30]. Furthermore, the dynamic nature of MIoT networks, where devices can join and leave frequently, demands continuous adaptation and updates to address the changing network environment, complicating the implementation of consistent and reliable security protocols [8]. Overcoming these challenges requires continuous research and development of adaptive, scalable security solutions [33]. Integrating AI-based protocols and anomaly detection mechanisms presents promising avenues for enhancing the resilience of MIoT ecosystems against sophisticated cyber threats in real-time, significantly reducing the risk of data breaches [1,31]. Additionally, simulation studies have been crucial supportive technologies in validating these cyber security measures, providing detailed insights into their performance under various scenarios and helping to identify potential weaknesses and areas for improvement [1,29,30].

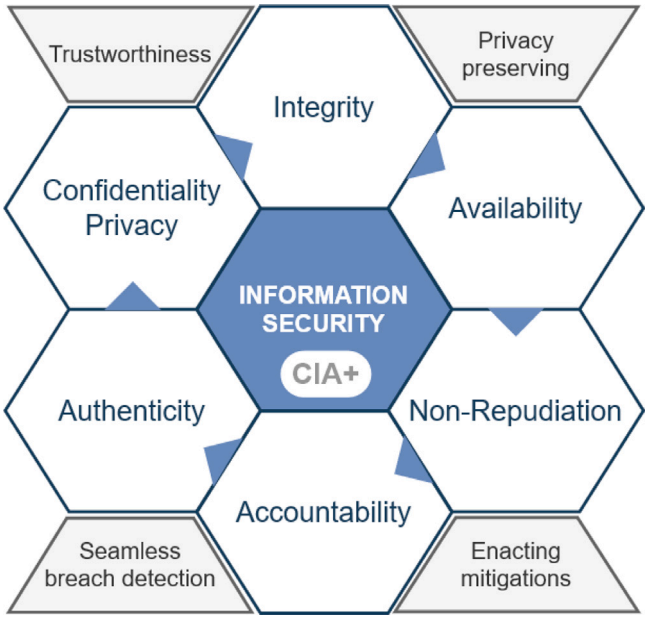


Fig. 1. Core cyber security dimensions and objectives in systems infrastructure.

Fig. 1 displays the core principles of cyber security, which are essential for protecting systems from cyber threats. These principles incorporate traditional CIA triad [34] and other dimensions such as *Authenticity* (verifying identities against access controls), *Privacy* (protecting personal data and controlling access to sensitive information), *Non-Repudiation* (ensuring actions are uniquely attributable to individuals), and *Accountability* (ensuring responsibility for actions). Together, they address critical areas in information security, providing the necessary attributes and assurances to strengthen systems against cyber-attacks.

Bhuiyan et al. (2021) [35] explored enabling technologies, security aspects, and market opportunities in MIoT, highlighting the need to expand beyond CIA concerns, particularly for MIoT devices communicating over the Internet. This expanded security framework, which we refer to as CIA+, requires security managers to balance the integration of these dimensions with budget constraints to ensure smooth operations. Continuous monitoring is crucial for maintaining service quality, auditing infrastructure for abnormalities, and ensuring accountability for potential perpetrators.

Improper controls at the infrastructure level in healthcare can expose patients and their medical data to significant risks unless best practices, industry standards, and vendor and community recommendations are followed. Common cyber-attacks affecting MIoT systems include Man-in-the-Middle (MitM), Distributed Denial-of-Service (DDoS), malware and data exfiltration [36,37]. These attacks on patients' smart devices can leak sensitive information to hackers and propagate to other interconnected devices, such as personal computers and hospital networks. A typical IoT infrastructure consists of multiple layers, each with distinct responsibilities: Application, Transport, Network, Data Link, and Physical layers. While this architecture and infrastructure are beyond the scope of this paper, extensive literature is available on the subject [38–42].

Recent studies reviewed advancements in security for MIoT systems [43], outlining effective measures and best practices to tackle the aforementioned cyber security challenges [21,43,44]. Malamas et al. (2021) [44] specifically focused on risk assessment methodologies, providing frameworks for evaluating and mitigating threats. In addition, research efforts have identified the challenges in managing evolving cyber security threats exploring how to use security recommendations and standards when integrating risk into modern development practices like DevOps [45].

Moreover, predicting and differentiating cyber-attacks from abnormal (or incompetent) use remains particularly difficult. Simulation-based technology helps mitigate these shortcomings, being a powerful approach to model scenarios, uncover complexities, and reveal potential vulnerabilities within MIoT systems [6,8,9,24,27].

2.1. Assessing MIoT cyber security using simulation techniques

Analysts working with MIoT infrastructure have been using simulation-based technology as a valuable approach to test and evaluate security strategies. These simulations show promise in enhancing cyber security by modelling and predicting various types of attacks [46], yet significant gaps remain. Much of the experiments occur in controlled environments that may not fully capture the complexity and variability of real-world MIoT deployments [29,30]. Recent work from 2020 to 2024 have increasingly applied simulation techniques, such as machine learning [28,47], encryption schemes [29,48], and anomaly detection [49], to address key challenges like data privacy [47], threat detection [28,47,49], and resource constraints [30,46,50] in MIoT environments. Table 1 shows recent studies in MIoT cyber security, highlighting their approaches and applied simulation tools.

Table 1
Current simulation-based approaches for analysing MIoT cyber security.

Authors	Research objectives	Simulation tools
Jyotheeswari and Jeyanthi (2020) [29]	Develop a hybrid encryption model for managing data security in MIoT	OpenSSL, Python library (cryptography)
Park et al. (2020) [50]	Lightweight framework to develop authentication and key agreement scheme for MIoT	OpenSSL, CP-ABE library
Kamarei et al. (2023) [46]	Develop a framework to secure MIoT systems against malicious and benign congestion	NS-2.35 simulator
Sankaran et al. (2023) [47]	Framework for secure M-Trust privacy protocol for MIoT in smart healthcare systems	MATLAB, AI-based modules
Aversano et al. (2024) [49]	Develop a framework to detect anomalies in synthetic MIoT traffic using machine learning	Scikit-learn, TensorFlow
Ioannou et al. (2024) [28]	Develop a green and effective machine learning intrusion detection system for MIoT	TensorFlow, energy- efficient models
Zhang et al. (2024) [48]	Framework to enhance secure attribute-based dynamic data sharing with efficient access policy hiding and updating for MIoT	Eclipse IDE with Type A1 pairing from JPBC
Nagarajan et al. (2024) [30]	Establish a robust defence against intrusion attempts and still trust in edge networks for MIoT	NS-3 simulator
This paper's contribution	Develop a dynamic risk assessment simulation-based framework for analysing cyber security events in MIoT and assist in threat analysis	Discrete-event Simulation (Arena® Simulation), threat modelling

Jyotheeswari and Jeyanthi (2020) [29] employed Python cryptography library and OpenSSL to simulate a hybrid encryption model for data security in MIoT. Using a different technology, Zhang et al. (2024) [48] leveraged Eclipse IDE with Type A1 pairing from JPBC to simulate attribute-based encryption schemes, focusing on secure data sharing and policy updating. Park et al. (2020) [50] used OpenSSL and CP-ABE library to simulate a lightweight authentication and key agreement scheme, enhancing authentication efficiency. These simulations present both limitations and opportunities for further refinement and optimisation through more holistic security risk assessments considering the evolving threats to MIoT environments.

Sankaran et al. (2023) [47] used MATLAB with AI-based modules to simulate a secure M-Trust privacy protocol to improve data privacy and reduce unauthorised access incidents, an essential aspect of user protection. Despite this, using MATLAB does not fully capture event-driven interactions and dependencies between entities as effectively as a DES approach, and it requires additional development to address a broader range of cyber security threats.

Aversano et al. (2024) [49] applied Scikit-learn and TensorFlow to simulate anomaly detection in synthetic Medical IoT traffic, achieving high accuracy in identifying and explaining anomalies. It is worth mentioning that synthetic data provides flexibility to test various scenarios and is useful for initial testing and model validation. Likewise, synthetic data plays a crucial role in demonstrating model requirements and outlining the steps involved in our dynamic risk assessment approach.

Ioannou et al. (2024) [28] used TensorFlow, however, in energy-efficient models to simulate a green machine learning intrusion detection system. In another important direction, Kamarei (2023) [46] used NS-2.35 to simulate congestion scenarios in IoT-based healthcare systems, focusing on mitigating both malicious and benign congestion. A common characteristic of these simulation models is their high specialisation and reliance on specific setup and parameterisation. However, their approaches could complement a broader dynamic risk assessment framework, which could integrate hybrid simulation techniques for a more proactive and comprehensive cyber defence.

Nagarajan et al. (2024) [30] employed NS-3, a discrete-event network simulator designed for research and education. The authors simulated internet protocols and network behaviours, explaining detailed models for various network scenarios and making them ideal for trust management and edge network security simulations. While effective in modelling specific network scenarios, their approach lacks the adaptability needed to address evolving and dynamic cyber threats in real-time.

The differences in simulation approaches highlight the diverse methodologies employed to enhance MIoT cyber security. Network simulators like the Network Simulator (NS) enable detailed simulation of network protocols and behaviours, essential for managing trust and security in networked environments. Each simulation tool offers distinct advantages; for instance, MATLAB and TensorFlow simulations provide sophisticated environments for developing and testing AI-based security protocols and anomaly detection systems, essential for proactive cyber security measures. Simulations using Eclipse with JPBC and Python's libraries focus on ensuring data integrity and secure communications, addressing specific encryption and authentication needs. Meanwhile, those using Discrete-event Simulations (DES), such as NS (on different versions), Arena® Simulation Software [51] and Simul8 [52], excel at modelling detailed interactions and event-driven processes, making them ideal for simulating real-world behaviours and evaluating the effects of dynamic threats. Integrating diverse simulation approaches into a comprehensive and effective cyber security framework requires leveraging the capabilities of each approach to address the multifaceted challenges safeguarding MIoT environments.

Each simulation approach offers specific advantages but also presents drawbacks and limitations. NS is well-suited for detailed network simulations but lacks the flexibility required for broader cyber security applications beyond protocol and network behaviour

analysis. Despite their powerful capabilities for developing sophisticated algorithms, MATLAB with AI modules and TensorFlow are resource-intensive and may be less suitable for environments with limited computational power. With JPBC and Python's libraries, Eclipse IDE focuses primarily on data security and encryption but may fail to address comprehensive threat detection and real-time response mechanisms. Although these tools are effective within their specific domains, they often do not provide the holistic view needed for MIoT cyber security. Our approach addresses this gap by advocating for a process-oriented DES, which offers a lightweight, flexible framework for simulating workflows and processes. It is ideal for assessing system efficiency and resource use in MIoT environments, complementing the network-specific focus of tools like NS-3 and remaining flexible enough to incorporate other security models and threat data as input.

3. A conceptual approach to dynamic risk assessment

Risk Assessment involves investigating potential vulnerabilities, the likelihood of cyber-attacks, and their potential impact on systems [53–56]. As discussed in previous work [21], numerous challenges exist when tackling dynamic and emergent situations in a cyber security context. Our focus has been on MIoT, discussing the importance of continuously monitoring the cyber health of systems for timely updates on potential risks. This research highlights the need for improved simulation models that allow analysts and developers to anticipate cyber security issues before systems are deployed in real-world operational settings [57].

Our dynamic risk assessment (DRA) framework follows a structured six-step approach to evaluate and mitigate cyber security risks in MIoT environments. Fig. 2 illustrates our approach, showing the sequential flow (Steps-I to VI) from data collection, preprocessing, and simulation scenarios proposition, eventually leading to actionable security recommendations. This process enables continuous monitoring and adaptation to new threats, using a dynamic and proactive approach to cyber security risk management.

- Step-I begins with collecting cyber security-related data from multiple sources (streams), such as network traffic, application/device logs, and threat intelligence feeds, to name a few possibilities.
- Step-II involves data preprocessing and deduplication to ensure that only accurate, non-redundant information is used in the analysis.
- Step-III parameterises the simulation model using the cleaned data, configuring key variables like resources, time to process entries, and arrival/departure patterns. Particularly to cyber security, data informing connection requests, data transfers, user creation/deletion, or configuration changes (to mention a few) could inform abnormal behaviours typical of malicious adversaries.
- Step-IV executes multiple simulation scenarios, testing various potential cyber security events, such as Denial-of-Service attacks, i.e., scenarios we aim to better understand in our study.
- Step-V aggregates the outputs from these scenarios and evaluates them based on predefined metrics, including system resilience, data integrity, and response times. In our THC case study, we illustrate the resource utilisation index as a metric for investigating overall capacity and identifying overuse, serving as a means for taking action to balance the system effectively.
- Step-VI generates a comprehensive report for decision-makers and stakeholders, with actionable recommendations for improving the system's security posture based on the simulation insights. This process enables continuous monitoring and adaptation to new threats, providing a dynamic and proactive approach to cyber security risk management.

These steps allow for understanding the problem and reason about how simulation-based approaches could help improve cyber security in MIoT for specific events, namely availability concerns and resource overuse (potentially due to unwarranted cyber-attacks. Analysts could refine models using the latest monitoring and incorporate them into the cycle described by our methodology for more accurate results and decision-making capabilities.

We selected a synthetic case study as our research strategy to enable a detailed examination of specific operational events [58] within the framework proposed. This simulation-oriented approach allowed us to simulate and analyse cyber security incidents to demonstrate the practical application of each step of our proposed framework.

3.1. Cyber security events in MIoT networks: a simulation study

This section introduces a synthetic Case Study to illustrate and discuss a model proposition that can serve as a baseline model for evaluating MIoT environments and scenarios by instantiating the different elements composing the 'real-world' and defining key model parameters and data. The model enables the simulation of multiple scenarios. Its primary objective is to identify potential shortcomings and explore alternative solutions.

> **Telehealth Hospital Centre (THC) Case Study:** Suppose THC is a fully integrated synthetic smart hospital located in a densely populated urban area, serving a population of nearly 1 million residents. THC employs 50 Medical Doctors (MDs), 95 nurses, and 100 support staff, with a capacity of 250 beds, and operates in three shifts: (i) from 1 am to 7 am, (ii) from 7 am to 3 pm, and (iii) from 3 pm to 1 am. Regarding daily attendance, THC handles about 2000 daily occurrences distributed across Accidents & Emergency (A&E), Intensive Care Units (ICU), and pre-scheduled surgeries.

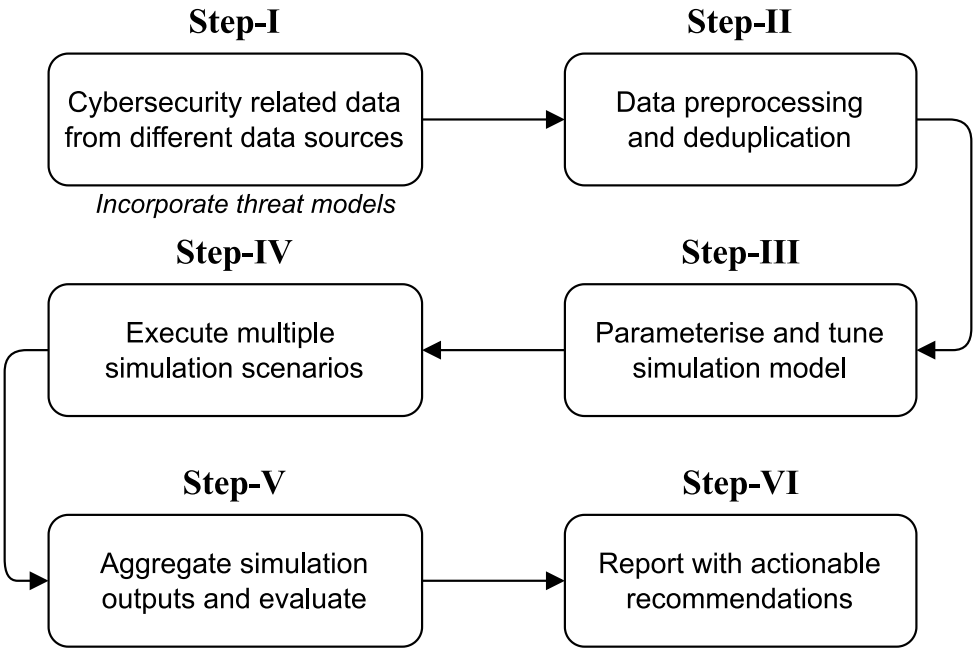


Fig. 2. Intertwined simulation within DRA approach proposition.

Upper management has made significant investments to transition THC into a smart telehealth hospital, leveraging extensive MIoT technology across its premises, staff, and patients. The goal is to remotely monitor hospital operations seamlessly, using low-cost sensors throughout the setting and transmitting data over secure networks. The managers acknowledge the vital role of cyber security, recognising it as a key factor in building stakeholder trust and driving greater efficiency when interacting with medical equipment and workflows and enhancing overall patient experience. Before investing, managers chose to model and simulate scenarios with virtual staff and patients to understand better challenges, focus efforts, and allocate resources efficiently. This cost-effective, low-risk approach demonstrated its value by revealing potential shortcomings and comparing various outcomes. In addition, integrating MIoT devices expands the hospital's attack surface, escalating concerns about cyber security threats that could compromise the integrity and privacy of operations.

3.1.1. Mapping key actors and attack surface in MIoT environments

Typically, cyber security measures and systems are in place; however, upper management has determined that these alone are insufficient to ensure a fully secure and trustworthy operation in a dynamic smart hospital environment. Recognising the complexity of the infrastructure, they have made substantial investments in building redundant services, allowing analysts to obtain a real-time, comprehensive operational overview via a dedicated Security Operations Centre (SOC). This SOC is continuously supplied with data from a vast array of MIoT devices and sensors distributed throughout the facility, which monitors every aspect of the hospital's operations. These sensors generate near real-time alerts, enabling responsible personnel to promptly identify and respond to potential threats. The infrastructure allows for the automatic execution of responsive tasks across interconnected systems and services, ensuring proactive risk management and operational resilience. We have identified the following key *general actors* in THC settings:

- **Medical staff** - includes doctors, nurses, and medical assistants directly involved in patient care.
- **Support staff** - encompasses technicians, maintenance teams, response teams, and IT administrators responsible for the hospital's technical and operational support.
- **Upper management** - comprises the Chief Executive Officer (CEO), Chief Scientific Officer (CSO), Chief Technology Officer (CTO), and Chief Information Security Officer (CISO), who oversees hospital management in a holistic/strategic fashion and makes decisions in line with budgetary constraints.

We list the following potential *equipment* within THC's context:

- **Wearable technologies** - a range of MIoT devices, including blood pressure monitors, smartwatches, electrocardiogram (ECG) trackers, and other biosensors such as heart rate monitors or sleep monitoring sensors.
- **Diagnostic machinery** - MIoT-enabled devices used for remote management, such as Magnetic Resonance Imaging (MRI) machines, X-ray machines, ultrasound devices, and mammography systems.

- **Hospital equipment** - other essential hospital equipment not previously mentioned, including vital signs monitors, wheelchairs, hospital beds, surgical tables, centrifuges, sterilisers, and ventilators. These are critical auxiliary devices that sustain daily operations and require continuous monitoring for failures or performance metrics.
- **Information and Communication Technologies (ICT)** - systems that support hospital operations, including Information Systems (IS) for data storage and retrieval related to hospital management, patients, and staff. These systems aim to ensure smooth operations, enabling investigations to take place (i.e., resolving specific incidents or anomalies, such as a suspected security breach), audits (i.e., systematic reviews or evaluations to ensure compliance with standards or policies), and forensic examinations (i.e., detailed data examination to reconstruct events, often after an incident) as needed.

As healthcare systems become increasingly interconnected and relying on smart technologies, the risk of cyber threats is a growing issue [59,60]. It is crucial to recognise threat actors that can exploit vulnerabilities in these systems, compromising both patient data and hospital operations. It is worth mentioning that both *internal* and *external* actors can exploit system vulnerabilities in a smart hospital setting. The following threat actors are particularly relevant in healthcare environments, and we introduce them in this THC case study:

- **Insiders** - Malicious system administrators or staff members with legitimate credentials to access key systems and patient data. In the THC context, they could manipulate or steal data, disrupt services, or disable security measures from within.
- **Disgruntled employees** - Former staff member who may still have access credentials, posing a significant risk to the hospital. Following an unamicable departure, these individuals might launch cyber-attacks or engage in other malicious activities to retaliate against the hospital.
- **Visitors** - While typically family members of patients, adversaries may disguise themselves as visitors. In a hospital such as THC, they can bring their own devices, potentially scouting for vulnerabilities in surveillance, access points (APs), or network infrastructure. Their physical access to the premises allows them to install malware, disrupt communications, or sabotage critical equipment.
- **State-sponsored agents and cyber-terrorists** - These actors launch sophisticated cyber-attacks aimed at weakening the hospital's capabilities by exploiting vulnerabilities. In the THC case, they could be considered Advanced Persistent Threats (APT) employing Living Off the Land (LOTL) to infiltrate and maintain long-term control over the hospital's infrastructure.
- **Industrial espionage actors** - Similar to state-sponsored agents, these actors could be competitors or third parties with an interest in the hospital's telehealth systems and MIoT technology. Their goal at THC would likely be data theft or exfiltration, such as patient records or proprietary operational information, among other cyber-attacks.
- **Script kiddies** - Inexperienced hackers who use pre-made scripts or tools from the Internet/Dark Web to attempt attacks. Although less skilled, these individuals could still disrupt THC's systems by exploiting basic vulnerabilities or conducting (Distributed) Denial-of-Service (DoS/DDoS) attacks, testing the hospital's cyber security defences.

The setting is highly dynamic, with new devices frequently entering and unpredictably leaving the infrastructure. Each device has its protocols, technology stack, and unique characteristics that must be accounted for in a comprehensive analysis. By mapping stakeholders, devices, threat actors, and equipment, we establish a foundation for integrating these elements into a simulation model, which is explored in the next subsection.

3.1.2. Understanding the data flow in hospital MIoT environments

We are modelling the flow of data units across hospital systems. Fig. 3 provides an overview of the data flow within hospital MIoT settings, illustrating the potential sources from which various systems generate data. At the centre, the SOC dashboards aggregate and display critical information, enabling a wide range of stakeholders to monitor system health and communications. The figure highlights key components such as Information Systems, Security Information Systems, External Data Sources, Data Consumption, and Data Sink, all interconnected to ensure seamless data management.

Given that numerous systems produce data within hospitals, our modelling effort focuses on the two highlighted triangles, where cyber security data is generated and consumed. It is worth mentioning that any data reaching the 'Dashboard @SOC' (refer to Fig. 3, the central component) is subject to a host of attacks namely data integrity, MitM, or availability attacks (to mention some), that aim to disrupt systems based on adversaries' objectives. In this sense, employing anomaly detection and conducting evaluations against historical data (before enabling data consumption to stakeholders) could help in identifying such issues and mitigating these attacks effectively.

Data from various systems offer analysts a comprehensive panorama of potential issues that require attention. The goal is to connect all these data sources into a centralised facility, where multiple dashboards display critical information about the system's health and communication. Stakeholders can access key data and alert systems, filtering significant events to focus their attention and respond effectively.

Regarding cyber security related data, firewall logs and access data can be integrated with a Security Information and Event Management (SIEM) system and Intrusion Detection System (IDS) outputs, which monitor user activity and data transfers. Additionally, external sources such as vulnerability catalogues, for instance, the US's National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE), and scoring systems such as the Common Vulnerability Scoring System (CVSS), along with expert commentary, can improve the understanding of ongoing threats, especially from sophisticated attackers.

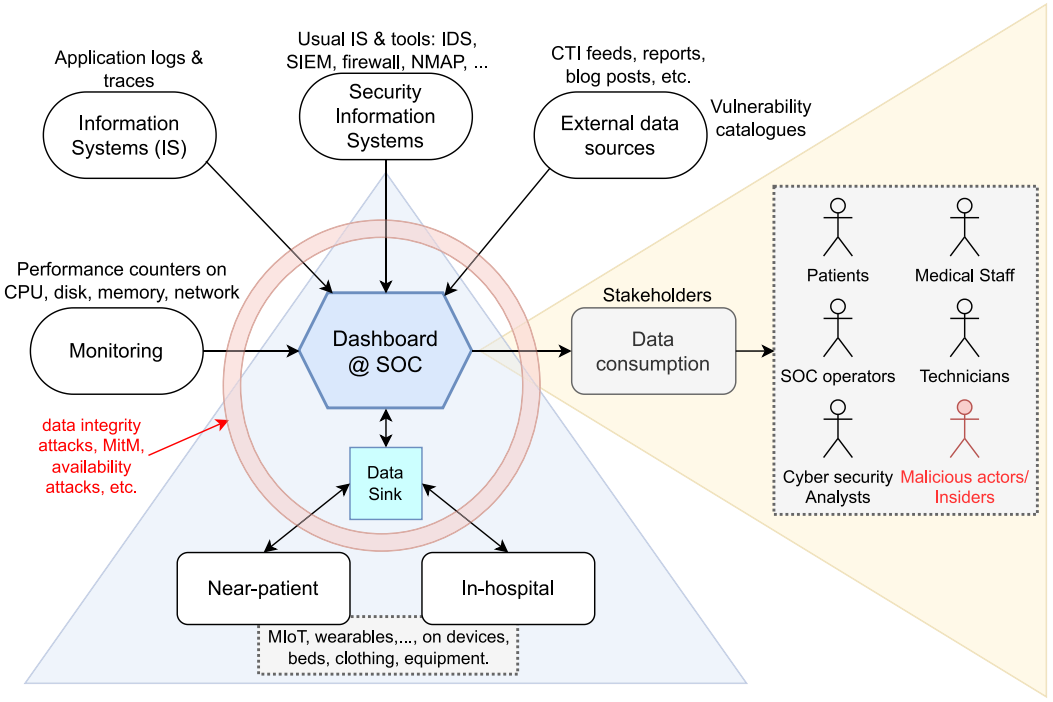


Fig. 3. Overview of data flow within hospital MIoT settings, key systems and devices.

The Data Sink component aggregates and processes information from MIoT devices across the hospital infrastructure, collecting time-series data from near-patient and in-hospital sources. These sources include MIoT devices, wearables, medical equipment, and beds-feeding, all of which contribute to the Data Sink's ability to centralise critical data for further analysis and monitoring. Before reaching the SOC dashboards, this data undergoes validation to remove duplicates and invalid entries. This process provides stakeholders with a near real-time snapshot of the dynamic attack surface, ensuring they can prioritise mitigation efforts efficiently when required.

Additionally, the figure shows the interactions between various actors (such as medical staff, SOC operators, and potentially malicious insiders), and the system, illustrating the importance of a robust cyber security framework to safeguard hospital operations and ensure data integrity.

3.1.3. Threat modelling for hospital settings and data security

Threat Modelling (TM) is a crucial activity that involves a comprehensive risk assessment of systems, offering a structured approach to evaluating system designs while considering cyber security trade-offs [54]. Shostack (2014) [61] outlined the TM process by posing four essential questions: (1) *What are we working on?*, (2) *What can go wrong?*, (3) *What are we going to do about it?*, and (4) *Did we do a good enough job?*. These questions guide the evaluation and mitigation of potential risks within the system.

Focusing on system implementation, Tarandach and Coles (2020) [62] defined it as *"the process of analysing a system to look for weaknesses that come from less-desirable design choices"*. Several important techniques have been developed to support this process, including STRIDE [61], PASTA [53], LINDDUN [63], Attack Trees [64,65], Persona non Grata, Security Cards, hTMM (Hybrid TM Method), Quantitative TMM, Trike, VAST (Visual, Agile, and Simple Threat) Modeling, INCLUDES NO DIRT [62], SPARTA, CORAS [66], among others [62,67]. More recently, Ekstedt et al. (2023) [55] introduced Yacraf (Yet Another Cyber security Risk Assessment Framework), which focuses on organisational decision-making capabilities through comprehensive risk assessments.

TM aligns with the goals of our study, as we address potential vulnerabilities arising in MIoT networks and frequent data exchanges. In this context, one technique particularly suited to these challenges is the use of Data Flow Diagrams (DFD) [68],[1] which help visualise and assess data movement within the system, and identify potential security risks at various stages.

Fig. 4 illustrates one (out of many possible) threat model that focuses on capturing the process of how patients and administrators log into an information system to retrieve and update reports, respectively. It highlights potential vulnerabilities in the authentication process for both user types and shows how data flows among processes, while also pointing to potential cyber-attack scenarios involving different adversaries, such as malicious insiders or hackers. A system of this scale (i.e., THC hospital system) not only contains multiple sub-systems but is also inherently complex, with various threat models arising from user interactions. The purpose

[1] Link for DFDv3: https://github.com/adamshostack/DFD3.

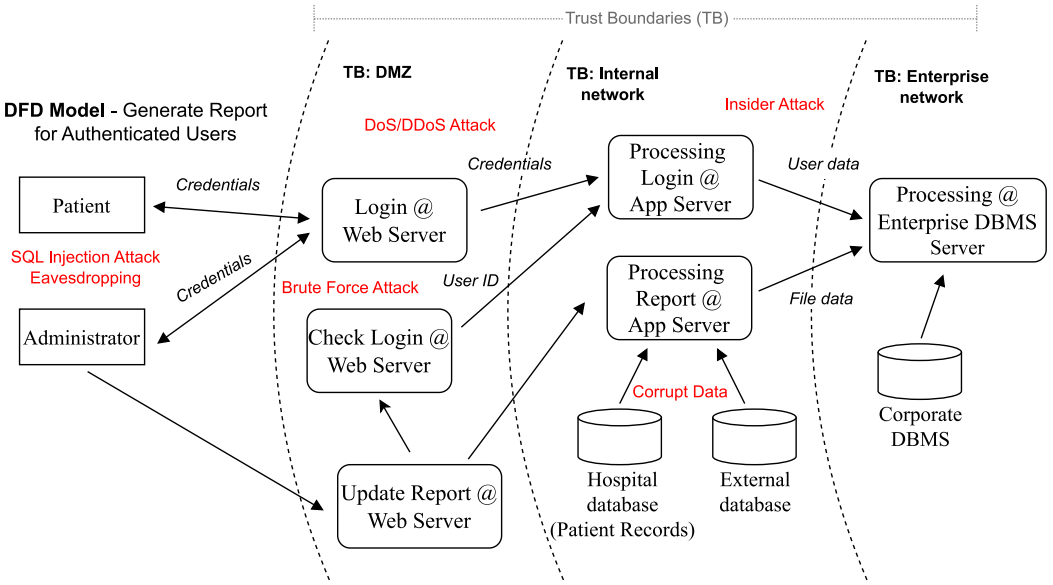


Fig. 4. Threat model for manipulating patient reports for authenticated users.

is twofold: first, to provide insights into potential attack vectors targeting underlying systems, and second, to inform our simulation model on how data flows between sub-systems and key servers.

Additional threat models could further complement this one by addressing scenarios such as: (i) generating patient data and transmitting it to the Data Sink; (ii) retrieving data from external (and complementary) systems and integrating it into local data systems (e.g., dashboard); and (iii) authenticated users accessing and consuming data over a specific time period. This list is non-exhaustive, as many more threat models would need to be developed by security analysts throughout the project to strengthen security defences and mitigation strategies comprehensively.

In summary, threat models can help various stakeholders (such as managers, security officers, and system administrators), in reasoning about how systems might be vulnerable to cyber-attacks and developing appropriate mechanisms for mitigation and hardening. In our simulation approach, these threat models can be used to inform the 'What-If' scenarios and produce simulation outputs that analysts can use to guide proactive and informed responses. The integration of DFDs into Step-I of our methodology (Fig. 2) provides a structured approach to mapping data flows, which strengthens the simulation's ability to represent potential threats and vulnerabilities within the system. This approach provides a comprehensive understanding of data exchanges and locates areas where security risks may emerge.

3.2. Simulating key cyber security events in MIoT systems

To guide effective protections, it is essential to address potential 'under attack' scenarios in MIoT networks. A key challenge is distinguishing between common network abnormalities, such as intermittent behaviours, and active cyber-attacks intended to disrupt the platform or damage connected devices. In the context of our THC case study, simulating key cyber security events in MIoT systems enables us to identify how various attacks exploit vulnerabilities in interconnected medical devices and hospital networks.

Before discussing the simulation, Fig. 5 presents the fundamental concepts to understand the attack surface of the THC case study. This visualisation helps to conceptualise how actors, threat agents, and security practices interact, guiding the identification of vulnerabilities and informing a broader DRA in the hospital's MIoT environment. It showcases a typical cyber security analysis of the organisation, where Modelling & Simulation approach could be used to present analysts with 'What-If' scenarios, capturing system overloads or under capacity conditions, among others. It also highlights the role of best practices, cyber security awareness, continuous monitoring, and SOC dashboards in maintaining CIA+ throughout the process.

The core idea of our approach is to gather synthetic or real data from MIoT, process it to remove duplicates or invalid entries, parameterise the simulation model, and run the model to identify potential cyber security issues in these networks. This builds on our previous research on Dynamic Risk Assessment (DRA) in healthcare [21], which addressed challenges posed by MIoT in dynamic networks.

Our framework adopts a holistic approach to the cyber security challenges faced by patients and hospitals, the end-users of smart device applications. Enacting these capabilities involves training users and administrators to grasp security concerns and report issues to security analysts for timely mitigation. These key elements, such as data processing and parameterisation, are essential for supporting the initial considerations and abstractions for the simulation model.

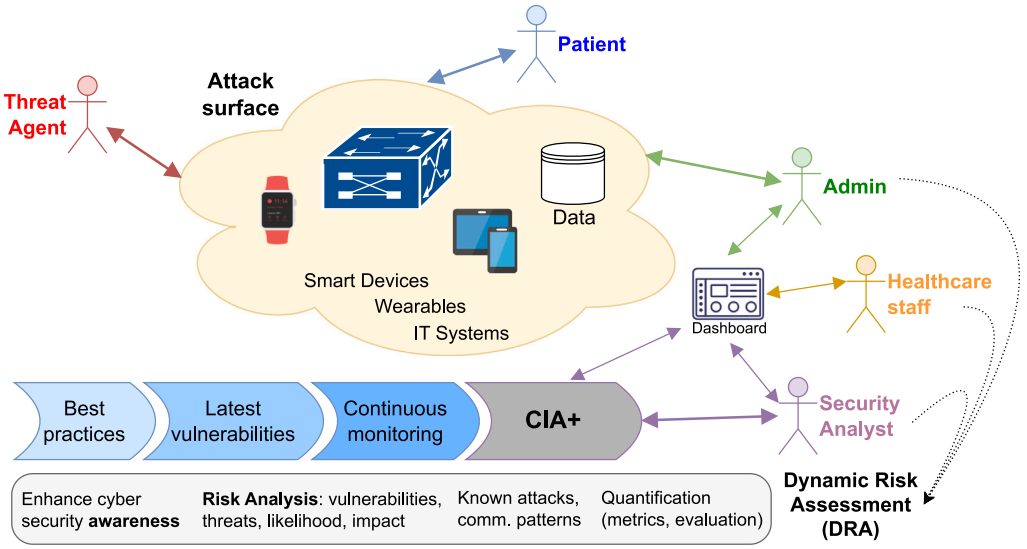


Fig. 5. Understanding attack surface in the THC case study.

For the purpose of demonstration and validation of our approach, we used the Arena® Simulation Software [51], by Rockwell Automation,[2] to model and simulate the THC Case Study using Discrete-event Simulation (DES) concepts. It is noteworthy that Arena® has been used for modelling various problems across application domains [69,70]. Using DES allows us to model systems behaviour as a sequence of discrete events over time. Each event occurs at a specific point, and the system transitions between states based on these events. A key concept in DES includes 'Entities' (representing elements like patients or devices), 'Activities' (actions or processes in the system), 'Resources' (elements needed for activities, such as staff or equipment), and 'Queues' (waiting lines for resources). Parameters like arrival rates, service times, and distributions are used to define how entities move through the system. Understanding these basic concepts is essential for parameterising our simulation model for MIoT analysis. For more background on DES concepts, please refer to Rosseti (2015) [51].

Table 2 presents the operational details for running the hospital, i.e., the total staff assigned to fulfilling its business objectives (MD, Nurse, IT administrators, Security officers, and Response teams), as well as equipment (beds, wearable, machinery, systems, etc.) over three shifts (per day analysis). The column Total shows the amount of resources available in the system at any point during the simulation, corresponding to the resource provisioning required to meet the modelled patient demands. The column %SOC represents the proportion of resources (divided across three shifts) actively monitoring the dashboard's alert system and making decisions. The attributes of each element are also defined, as they will be reflected in the simulation output plots (in Fig. 7). These parameters were used in the simulation 'Run Setup' options within Arena®. The model operates on a 24-h clock, simulating one day (1440 min) divided into the three detailed shifts.

For this case study, we specifically simulate data processing requirements to ensure the SOC dashboard is supplied with accurate information for stakeholders, both in *normal* conditions and *under attack*, where adversaries inject spurious data or corrupt it during transit or while at rest. Furthermore, our system abstraction operates under the following assumptions:

- We focus exclusively on 'noticeable cyber security events' from the MIoT device network, prioritising data from patient monitoring devices, though other sources like security information systems and equipment sensors also reach the SOC dashboard.
- A device is modelled as either 'normal' (functioning as expected) or 'compromised with malware', meaning it generates and transmits incorrect data that deviates from expected patterns (e.g., size, payload, frequency, and other characteristics).
- Among the resources (listed in Table 2), only a subset is allocated to handling MIoT-related cyber security events through different interfaces, such as mobile apps or desktop applications with dashboards that display the devices (attached to patients) under their supervision.
- Column #Min. represents the total time (in minutes) per shift. During each shift, there are potential 'arrivals' of MIoT data (originating from both 'in-hospital' and 'in-patient' devices), which may generate noticeable cyber security events.
- We modelled arrivals using an exponential distribution with the parameter 'Total arrival/|Interval|' to capture the inter-arrival times, as required by the simulation software (where the operator $|\cdot|$ refers to the size or extent (length) of the 'Interval'). This distribution is well-suited for systems like these, where events occur independently over time, i.e., the probability of an event occurring in the future is independent of any previous events [51].

[2] Link: https://www.rockwellautomation.com.

Table 2
Initial considerations and abstractions for the THC MIoT system under study.

Hospital operational details		Total	%SOC	Attribute
Staff	Medical Doctor (MD)	50	4%	R_MEDIC
	Nurse	95	5%	R_NURSE
	IT admin	5	90%	R_TTEAM
	Security officer	7	50%	R_STEAM
	Response team	5	85%	R_RTEAM
		Total	%	
Equipment	Number of beds	250	30%	T_BEDS (0)
	Wearable technologies	500	60%	T_WEAR (1)
	Diagnostics machinery	25	3%	T_DIAG (2)
	Hospital equipment	50	6%	T_EQUI (3)
	ICT/IS equipment	10	1%	T_ICTS (4)

Shifts	Duration	Total arrival	#Min.	Interval	Attribute *(on entity)*
	01:00–07:00	500	360	[0;360]	T_1ST
	07:01–15:00	1500	480	(360;840]	T_2ND
	15:01–00:59	250	600	(840;1440]	T_3RD

Table 3
Assigning types according to arrivals on the system and involved resources.

Equipment (types)	Av.[a]	Ratio R	Factor F	R×F	U[b]	A[c]	Involved Resources
Beds (0)	250	30%	0.10	0.0299	0.26	0.26	R_MEDIC R_NURSE
Wearable (1)	500	60%	0.10	0.0599	0.52	0.78	R_STEAM R_RTEAM
Diagnostics (2)	25	3%	0.35	0.0105	0.09	0.87	R_TTEAM R_STEAM
Hospital (3)	50	6%	0.20	0.0120	0.10	0.97	R_TTEAM R_STEAM
ICT/IS (4)	10	1%	0.25	0.0030	0.03	1.00	R_TTEAM R_STEAM
Totals:	835	100%	1.0	0.1153	1.0	–	–

[a] Available units.
[b] Uniformisation of $R \times F$.
[c] Accumulated value.

Table 3 shows how we assign device type (in the simulation model) based on MIoT system arrivals, using uniformly distributed variables to determine the device type based on the number of devices, where each type has an equal probability of being selected.

The Ratio column computes the percentage of each device type relative to the total, normalising it based on the sum. Observe that we use a variable called Factor, i.e., 'Attack Factor', which assigns a value in the range [0;1], to map cyber security protections on devices and tackle situations where threat actors disrupt, corrupt, or abuse the equipment.

Lastly, column A⋆ applies this normalised value to assign device types using a random number drawn from a uniform distribution. For instance, if the value falls within [0.0; 0.26], it assigns a 'Bed' (all MIoT-enabled), and if between (0.26; 0.78], it assigns a 'Wearable' device, and so forth.

Table 3 also shows the resources allocated (mapped) for addressing occurrences. Note that 'Beds' and 'Wearable' involve all resource types, while technical teams handle the remaining equipment in cases of malfunction or unexpected behaviour.

3.3. THC case study model outline and parameterisation

Ideally, all queues, delays, capacities, inter-arrival times, and schedules would be derived from actual MIoT logs and data that monitor staff and equipment. Note that choosing the appropriate probability distribution is fundamental to any analysis. To overcome these limitations, such as the absence of real data, we will make *assumptions* and employ 'What-If' scenarios to assign the simulation parameters.

Fig. 6 shows the core concept of our model, which we simplified to showcase only the essential components of our approach, as the complete Arena® (DES) model on GitHub repository,[3] includes 10 'Seize-Delay-Release Queues', 6 'Resources', 8 'Variables', 13 'Assignments', and 11 'Decide' modules. In Arena® these concepts [51] are defined as follows: 'Seize-Delay-Release Queue', i.e., the

[3] Arena® (DES) model: https://github.com/czekster/dra-model-2024.

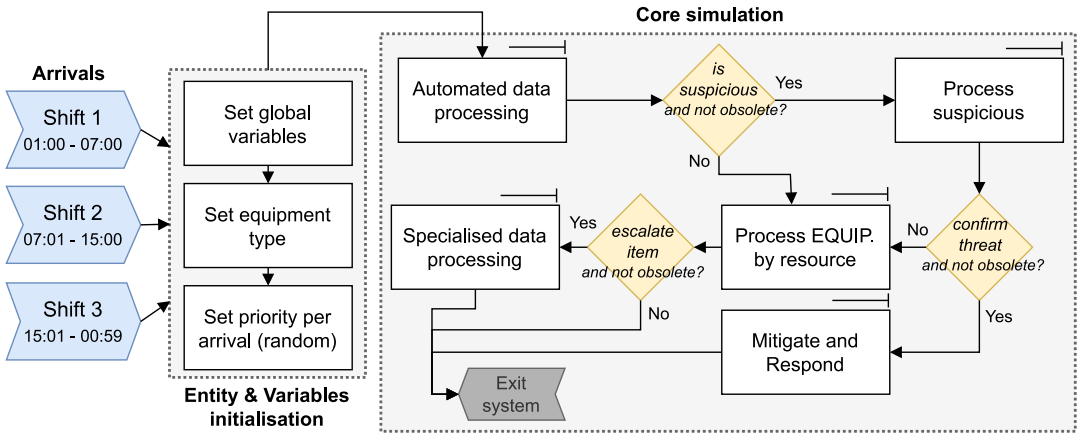


Fig. 6. Simulation model showing the main process for running the case study.

process where an entity seizes a resource (e.g., a device or staff), delays while performing an activity, and then releases the resource for others to use. 'Resources' are elements (equipment, staff) that entities need to carry out activities within the simulation. 'Variables' introduce data holders that store values which can change during the simulation (e.g., counters). The module 'Assignments' attributes new values to variables (or updates them) based on simulation events. The module 'Decide' allows the inclusion of decision points that direct the flow of entities based on conditions or probabilities, allowing for diverging paths in the simulation.

The approach begins by initialising the arriving elements ('Entities') with attributes and global variables (e.g., timeout and threshold). The core simulation then starts by processing data, which involves tasks such as collating, aggregating and removing duplicates, outliers and invalid entries; similar to the continuous work performed by the SOC throughout the day. The data entry is then inspected for obsolescence (based on the 'TIMEOUT' constant) or suspicious behaviour. If further analysis is required, the data is sent to processing units to confirm or refute potential threats. If no issues are found, the data proceeds with standard processing; otherwise, it is directed to mitigation (response teams).

Table 4 lists the parameters used in the simulation model. Analysts can adjust these parameters to adapt the model to different contexts or explore various behaviours. Additionally, we outline further modelling decisions for the simulation, particularly concerning device (equipment types) maintenance and prioritisation (the full model will be explained in later sections). All queues in Arena® are configured to select the next entity based on *Priority* attribute, determined by a random value drawn from a Normal Distribution expressed as NORM(50,20), with a mean of 50 and a standard deviation of 20. Activities present 'service times' represented by the TRIA(MIN,MODE,MAX) function, which denotes a 'Triangular' probability distribution in the simulation tool. Its parameters specify a minimum value, most likely value (mode), and maximum value, drawing random values within the range [MIN; MAX]. The triangular distribution is often used in simulations when there is limited sample data available, but these values are known or can be estimated [51]. The goal is to establish a threshold that processes high-priority entities first (this can be parameterisable).

We stress that conducting a 'What-If' scenario analysis is fundamental, especially for resource allocation and investment decisions (e.g., hiring more staff), to maintain a reasonable Quality-of-Service (QoS) for end-users while preventing operational staff from becoming overburdened, which could lead to underperformance or burnout.

Regarding cyber security considerations in the model, we use the explained 'Attack Factor' (refer to Factor in Table 3) to identify suspicious data. This mapping helps us understand our system's abstraction and focuses explicitly on MIoT data as it arrives, is validated, and is consumed within the system, indicating events potentially subject to cyber security violations.

3.4. THC case study model output detail

As mentioned, the strengths of the approach outlined in this work lie in providing a basic model that abstracts data flows within a healthcare setting and simulates MIoT operations involving various resources (see Table 2).

Regarding the soundness and expressiveness of the approach, the level of detail in the simulation model determines the analyses and variations available for consideration, which, e.g., analysts might consider. We believe our mapping serves as an initial modelling effort, valuable for upper management overseeing the complex attack surface of distributed MIoT, as well as for security analysts investigating potential cyber-attacks in such networks.

Fig. 7 illustrates the resource utilisation across all replications (i.e., independent runs of the simulation model to assess the variability of outcomes and provide more reliable estimates of performance measures [51]) representing the daily workload of key stakeholders managing the dashboards. In this experiment, we ran 10 replications, which showed a reasonable level of confidence in the simulation outcome (resource utilisation estimates). These results reflect the probability distributions assigned in the model; hence, analysts may adjust parameters to achieve suitable compromises that align with resources/budget constraints; one can also utilise advanced tools like Arena® OptQuest [51], which is a built-in feature of the simulation suite, to identify optimal configurations by systematically varying parameters.

Table 4
Arena® simulation parameters for 'What-If' scenario analysis.

Elements	Activities description	Probability distributions
Queues (Q)	Automated data processing	TRIA(0.5,1.0,1.5)
	Process suspicions	NORM(5,2)
	Process BED by nurse	TRIA(3,5,7)
	Process MIoT by MD	TRIA(6,7,10)
	Process WEARABLE by nurse	EXPO(2)
	Process DIAGNOSTIC by IT	UNIF(1,10)
	Process HOSPITAL by IT	UNIF(5,10)
	Process EQUIP by STEAM	UNIF(5,15)
	Process ICT by IT	UNIF(3,7)
	Mitigate & Respond	TRIA(9,11,15)

		Value if true
Choices	Escalate to MD?	50%
	Escalate to STEAM?	25%
	Is it suspicious?	[a]
	Confirmed threat?	25%
	Is it obsolete?	[b]
Q. Policy	Highest priority first	–
Constants	SUSP_THRESHOLD (perc)	25%
	TIMEOUT (min)	10
	SELECT_PRIORITY (value)	80

[a] UNIF(0,1) < SUSP_THRESHOLD.
[b] Time in system < TIMEOUT.

	Resource	Quantity
Capacities	MD	2
	Nurse	5
	IT admin	5
	Sec officer	4
	Resp team	5
	Auto-script	2

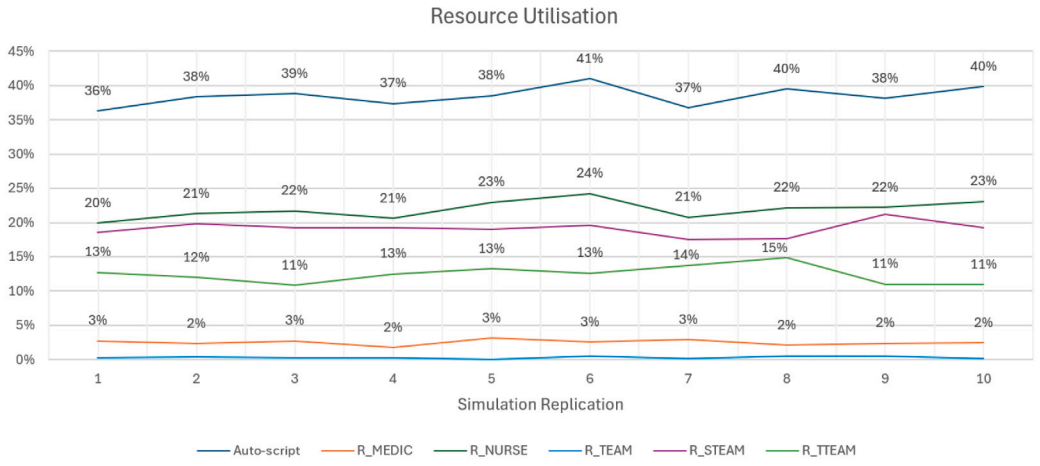


Fig. 7. Resource utilisation output across all simulation replications.

In this simulation exercise, a total of 5571 data items were processed, with 625 discarded due to obsolescence. Given the allocation of numerous resources, queue sizes remained minimal, allowing us to reduce the number of professionals in the model and observe the resulting impact on resource utilisation (Fig. 7), as changes in staffing levels affect overall system dynamics. It is important to highlight that this experiment was intended to demonstrate the potential of the simulation model as a parameterisable approach to evaluate different MIoT scenarios effectively. In addition, the synthetic case study aimed to reflect realistic conditions in MIoT environments, such as resource constraints, data flows, and cyber security threats. We intended to approximate the model to real-world MIoT operations, making its outcomes valuable for operational planning and risk assessment.

Our model provides security analysts with a base model template representing the MIoT infrastructure, enabling them to create multiple 'What-If' scenarios for timely analysis and output comparison. The simulation model is designed to be generic for IoT, addressing the need to manage data across large attack surfaces. With budgetary constraints in mind, it can be adapted to different contexts and scaled accordingly. Our DRA approach including simulation models informed by threat models, therefore, enhances the overall risk assessment process, offering an additional perspective on the dynamic interactions and potential threats within an MIoT system.

As Kaufhold et al. (2024) [24] pointed out, response teams engaged in cyber situational awareness face the challenge of managing multiple data sources feeding dashboards with status updates and incidents across extensive attack surfaces. Sometimes, capacity constraints can hinder the timely and adequate mitigation of cyber-attacks as they evolve within networks and systems. Our contribution aims to assist management in adjusting operational capacity through simulation, which provides insights into team composition and more strategic resource investment. The next step in this analysis is to vary the constants, variables, decision elements, resource allocation schemes, and fit probability distributions using real hospital MIoT data streams.

Additionally, we plan to study TM's integration into the simulation, building on our initial considerations to better structure scenario development. This will allow a more systematic evaluation of how threats impact resource allocation and system dynamics. The ultimate objective is to identify a scenario where resources can efficiently and promptly process data, ensuring high Quality of Service (QoS) and efficient hospital operations. Although the model was developed in Arena®, which contains built-in functionalities specifically designed for DES, similar capabilities can be achieved using Python libraries (e.g., SymPy, salabim). Analysts have the flexibility to use their preferred tool by learning its specific features or adapting our simulation model to fit their chosen platform.

Another important direction involves enriching our simulation models with data from Cyber Threat Intelligence (CTI) sources and incorporating this information into model parameters. We have previously explored aspects of this approach [71,72], which remains a hot topic in cyber security research, as evidenced by other relevant works [56,73].

4. Conclusion

Cyber-attacks continue to permeate MIoT networks as sophisticated threat actors engage in criminal activities to disrupt, abuse, steal, or corrupt healthcare systems. Over the years, security managers have documented and analysed the typical pathways attackers use to access systems, exfiltrate data, and perform lateral movements to inflict damage. However, raising awareness alone is insufficient; it must be coupled with continuous security monitoring, user and staff training, and secure programming practices, which inevitably increase budgetary demands and investments.

The approach presented in this work aimed to determine the mechanisms behind attacks (the 'how') and the motivations driving malicious activities (the 'why') through simulations, providing actionable insights for counteractions and mitigation. The idea was to examine potential weaknesses or shortcomings in systems through simulation models to understand how to enact effective protective measures. The dynamic aspect of the DRA approach was abstracted in the simulation model, where we considered emerging threats as they impact MIoT networks. In the future, we plan to study how to plug-in real-time data directly into the simulation model for timely analysis, which will help better capture the nuances and dynamics of progressing cyber-attacks. The framework described herein maps the critical segments of the MIoT attack surface, using modelling to identify vulnerabilities and guide mitigation strategies. The approach remains lightweight and cost-effective, requiring only a basic mapping of MIoT devices, their interconnections, and relevant operational parameters.

Finally, understanding cyber-attacks and malicious activities in MIoT environments remains a significant challenge for analysts. Therefore, we advocate for combining simulation-based approaches with other tools and resources, such as MITRE's ATT&CK Navigator,[4] to stay informed about emerging threats and security incidents in systems. Such a combination allows for a more comprehensive understanding of potential vulnerabilities and effective mitigation tactics. Additionally, risk assessment is a critical area of research that has seen significant contributions over the years. We believe that achieving near real-time analysis is paramount for understanding the progression of attacks and stymieing malicious incursions before they escalate, ultimately ensuring the security and resilience of MIoT systems.

Acronyms

A&E: Accidents & Emergency; **AP**: Access Point; **APT**: Advanced Persistent Threats; **CEO**: Chief Executive Officer; **CIA**: Confidentiality, Integrity, Availability; **CISO**: Chief Information Security Officer; **CP-ABE**: Ciphertext-Policy Attribute-Based Encryption; **CSO**: Chief Scientific Officer; **CTI**: Cyber Threat Intelligence; **CTO**: Chief Technology Officer; **CVE**: Common Vulnerabilities and Exposures; **CVSS**: Common Vulnerability Scoring System; **DBMS**: Database Management System; **DoS/DDoS**: Distributed Denial-of-Service; **DES**: Discrete-event Simulation; **DFD**: Data Flow Diagram; **DMZ**: Demilitarised Zone; **DoS**: Denial-of-Service; **DRA**: Dynamic Risk Assessment; **DT**: Digital Twins; **ECG**: Electrocardiogram; **hTMM**: Hybrid Threat Modeling Method; **ICT**: Information and Communication Technologies; **ICU**: Intensive Care Unit; **IDE**: Integrated Development Environment; **IDS**: Intrusion Detection System; **IoT**: Internet-of-Things; **IS**: Information Systems; **IT**: Information Technology; **JPBC**: Java Pairing-Based Cryptography; **LINDDUN**: Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance; **LOTL**: Living Off The Land; **MD**: Medical Doctor; **MIoT**: Medical IoT; **MitM**: Man-in-the-Middle Attacks; **MRI**: Magnetic Resonance

[4] Link: https://mitre-attack.github.io/attack-navigator/.

Imaging; **NMAP**: Network Mapper (tool); **NS**: Network Simulator; **NVD**: National Vulnerability Database; **OpenSSL**: Open Secure Sockets Layer; **PASTA**: Process for Attack Simulation and Threat Analysis; **QoS**: Quality of Service; **SIEM**: Security Information and Event Management; **SOC**: Security Operations Centre; **STRIDE**: Spoofing, Tampering, Repudiation, Information disclosure, DoS, Elevation of privilege; **THC**: Telehealth Hospital Centre; **TM**: Threat Modelling. **VAST**: Visual, Agile, and Simple Threat Modeling. **Yacraf**: Yet Another Cyber Risk Assessment Framework.

CRediT authorship contribution statement

Ricardo M. Czekster: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Thais Webber:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Methodology, Investigation, Formal analysis, Conceptualization. **Leonardo Bertolin Furstenau:** Writing – review & editing, Visualization, Validation, Supervision, Software, Methodology, Investigation, Formal analysis, Conceptualization. **César Marcon:** Writing – review & editing, Visualization, Validation, Supervision, Project administration, Methodology, Investigation, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Ricardo Melo Czekster reports financial support was provided by Brazilian State Funding Agencies (FAPs), articulated by its National Council (CONFAP), and the National Council for Scientific and Technological Development (CNPq). Cesar Marcon reports financial support was provided by Brazilian State Funding Agencies (FAPs), articulated by its National Council (CONFAP), and the National Council for Scientific and Technological Development (CNPq). If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

FAPERGS/RS/BRAZIL, Grant number: 22/2551-0001368-6.

Data availability

Data will be made available on request.

References

[1] R. Ahmad, M. Hämäläinen, R. Wazirali, T. Abu-Ain, Digital-care in next generation networks: Requirements and future directions, Comput. Netw. 224 (2023) 109599.
[2] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, K. Mankodiya, Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare, Future Gener. Comput. Syst. 78 (2018) 659–676.
[3] F. Alsubaei, A. Abuhussein, S. Shiva, Security and privacy in the internet of medical things: taxonomy andehealth risk assessment, in: 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), IEEE, 2017, pp. 112–120.
[4] Z. Ashfaq, A. Rafay, R. Mumtaz, S.M.H. Zaidi, H. Saleem, S.A.R. Zaidi, S. Mumtaz, A. Haque, A review of enabling technologies for internet of medical things (IoMT) ecosystem, Ain Shams Eng. J. 13 (4) (2022) 101660.
[5] A. Balasundaram, S. Routray, A. Prabu, P. Krishnan, P.P. Malla, M. Maiti, Internet of things (IoT)-based smart healthcare system for efficient diagnostics of health parameters of patients in emergency care, IEEE Internet Things J. 10 (21) (2023) 18563–18570.
[6] P.A. Williams, A.J. Woodward, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, Med. Dev.: Evid. Res. (2015) 305–316.
[7] L.M. Dang, M.J. Piran, D. Han, K. Min, H. Moon, A survey on internet of things and cloud computing for healthcare, Electronics 8 (7) (2019) 768.
[8] A. Ahmed, R. Latif, S. Latif, H. Abbas, F.A. Khan, Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review, Multimedia Tools Appl. 77 (2018) 21947–21965.
[9] S. Walker-Roberts, M. Hammoudeh, A. Dehghantanha, A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure, IEEE Access 6 (2018) 25167–25177.
[10] S. Zeadally, J.T. Isaac, Z. Baig, Security attacks and solutions in electronic health (e-health) systems, J. Med. Syst. 40 (2016) 1–12.
[11] B.A. Alahmadi, L. Axon, I. Martinovic, 99% false positives: A qualitative study of {SOC} analysts' perspectives on security alarms, in: 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 2783–2800.
[12] T. Ban, N. Samuel, T. Takahashi, D. Inoue, Combat security alert fatigue with AI-assisted techniques, in: Proceedings of the 14th Cyber Security Experimentation and Test Workshop, 2021, pp. 9–16.
[13] A. Yaseen, Accelerating the SOC: Achieve greater efficiency with AI-driven automation, Int. J. Responsib. Artif. Intell. 12 (1) (2022) 1–19.
[14] A. Villalón-Huerta, H.M. Gisbert, I. Ripoll-Ripoll, SOC critical path: A defensive kill chain model, Ieee Access 10 (2022) 13570–13581.
[15] M.Z. Nezhad, A.J.J. Bojnordi, M. Mehraeen, R. Bagheri, J. Rezazadeh, Securing the future of IoT-healthcare systems: A meta-synthesis of mandatory security requirements, Int. J. Med. Inform. 185 (2024) 105379.
[16] M.A. Sadeeq, S.R. Zeebaree, R. Qashi, S.H. Ahmed, K. Jacksi, Internet of things security: a survey, in: 2018 International Conference on Advanced Science and Engineering, ICOASE, IEEE, 2018, pp. 162–166.
[17] B. Bai, S. Nazir, Y. Bai, A. Anees, Security and provenance for internet of health things: A systematic literature review, J. Softw.: Evol. Process 33 (5) (2021) e2335.

[18] B. Liao, Y. Ali, S. Nazir, L. He, H.U. Khan, Security analysis of IoT devices by using mobile computing: a systematic literature review, IEEE Access 8 (2020) 120331–120350.
[19] I. Ali, A.I.A. Ahmed, A. Almogren, M.A. Raza, S.A. Shah, A. Khan, A. Gani, Systematic literature review on IoT-based botnet attack, IEEE Access 8 (2020) 212220–212232.
[20] I. Stellios, P. Kotzanikolaou, C. Grigoriadis, Assessing IoT enabled cyber-physical attack paths against critical systems, Comput. Secur. 107 (2021) 102316.
[21] R.M. Czekster, P. Grace, C. Marcon, F. Hessel, S.C. Cazella, Challenges and opportunities for conducting dynamic risk assessments in medical IoT, Appl. Sci. 13 (13) (2023) 7406.
[22] J.-P.A. Yaacoub, H.N. Noura, O. Salman, A. Chehab, Ethical hacking for IoT: Security issues, challenges, solutions and recommendations, Internet Things and Cyber-Phys. Syst. 3 (2023) 280–308.
[23] L. Bertolin Furstenau, T. Abreu Saurin, Designing resilient health services supported by digital technologies: A study of the blood transfusion process, Technol. Soc. 77 (C) (2024).
[24] M.-A. Kaufhold, T. Riebe, M. Bayer, C. Reuter, 'We do not have the capacity to monitor all media': A design case study on cyber situational awareness in computer emergency response teams, in: Proceedings of the CHI Conference on Human Factors in Computing Systems, 2024, pp. 1–16.
[25] H. Elayan, M. Aloqaily, M. Guizani, Digital twin for intelligent context-aware IoT healthcare systems, IEEE Internet Things J. 8 (23) (2021) 16749–16757.
[26] I. Al-Dalati, Digital twins and cybersecurity in healthcare systems, in: Digital Twin for Healthcare, Elsevier, 2023, pp. 195–221.
[27] M. Javaid, A. Haleem, R.P. Singh, R. Suman, Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends, Cyber Secur. Appl. (2023) 100016.
[28] I. Ioannou, P. Nagaradjane, P. Angin, P. Balasubramanian, K.J. Kavitha, P. Murugan, V. Vassiliou, GEMLIDS-MIOT: A green effective machine learning intrusion detection system based on federated learning for medical IoT network security hardening, Comput. Commun. (2024).
[29] P. Jyotheeswari, N. Jeyanthi, Hybrid encryption model for managing the data security in medical internet of things, Int. J. Internet Protocol Technol. 13 (1) (2020) 25–31.
[30] G. Nagarajan, M. Margala, P. Chakrabarti, R. Minu, et al., A trust-centric approach to intrusion detection in edge networks for medical internet of thing ecosystems, Comput. Electr. Eng. 115 (2024) 109129.
[31] J. Kaur, R. Verma, N.R. Alharbe, A. Agrawal, R.A. Khan, Importance of fog computing in healthcare 4.0, Fog Comput. Healthc. 4.0 Environ.: Tech. Soc. Future Implic. (2021) 79–101.
[32] H.A. Tarish, R. Hassan, K.A.Z. Ariffin, M.M. Jaber, Network security framework for internet of medical things applications: A survey, J. Intell. Syst. 33 (1) (2024) 20230220.
[33] A. López Martínez, M. Gil Pérez, A. Ruiz-Martínez, A comprehensive review of the state-of-the-art on security and privacy issues in healthcare, ACM Comput. Surv. 55 (12) (2023) 1–38.
[34] S. Samonas, D. Coss, The CIA strikes back: Redefining confidentiality, integrity and availability in security, J. Inf. Syst. Secur. 10 (3) (2014).
[35] M.N. Bhuiyan, M.M. Rahman, M.M. Billah, D. Saha, Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities, IEEE Internet Things J. 8 (13) (2021) 10474–10498.
[36] A. Djenna, D.E. Saïdouni, Cyber attacks classification in IoT-based-healthcare infrastructure, in: 2018 2nd Cyber Security in Networking Conference (CSNet), IEEE, 2018, pp. 1–4.
[37] S.P. Amaraweera, M.N. Halgamuge, Internet of things in the healthcare sector: overview of security and privacy issues, Secur. Priv. Trust IoT Environ. (2019) 153–179.
[38] P.K. Malik, R. Sharma, R. Singh, A. Gehlot, S.C. Satapathy, W.S. Alnumay, D. Pelusi, U. Ghosh, J. Nayak, Industrial internet of things and its applications in industry 4.0: State of the art, Comput. Commun. 166 (2021) 125–139.
[39] S. Razdan, S. Sharma, Internet of medical things (IoMT): Overview, emerging technologies, and case studies, IETE Tech. Rev. 39 (4) (2022) 775–788.
[40] K. Wei, L. Zhang, Y. Guo, X. Jiang, Health monitoring based on internet of medical things: architecture, enabling technologies, and applications, IEEE Access 8 (2020) 27468–27478.
[41] V.S. Naresh, S.S. Pericherla, P.S.R. Murty, S. Reddi, Internet of things in healthcare: Architecture, applications, challenges, and solutions., Comput. Syst. Sci. Eng. 35 (6) (2020).
[42] R. Dwivedi, D. Mehrotra, S. Chandra, Potential of internet of medical things (IoMT) applications in building a smart healthcare system: A systematic review, J. Oral Biol. Craniofac. Res. 12 (2) (2022) 302–318.
[43] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, R. Jain, Recent advances in the internet-of-medical-things (IoMT) systems security, IEEE Internet Things J. 8 (11) (2020) 8707–8718.
[44] V. Malamas, F. Chantzis, T.K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou, C. Douligeris, Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal, IEEE Access 9 (2021) 40049–40075.
[45] R.M. Czekster, Continuous risk assessment in secure DevOps, 2024, arXiv preprint arXiv:2409.03405.
[46] M. Kamarei, A. Patooghy, A. Alsharif, A.A.S. AlQahtani, Securing IoT-based healthcare systems against malicious and benign congestion, IEEE Internet Things J. (2023).
[47] K.S. Sankaran, T.-H. Kim, P. Renjith, An improved AI based secure M-trust privacy protocol for medical internet of things in smart healthcare system, IEEE Internet Things J. (2023).
[48] L. Zhang, S. Xie, Q. Wu, F. Rezaeibagha, Enhanced secure attribute-based dynamic data sharing scheme with efficient access policy hiding and policy updating for IoMT, IEEE Internet Things J. (2024).
[49] L. Aversano, M.L. Bernardi, M. Cimitile, D. Montano, R. Pecori, L. Veltri, Explainable anomaly detection of synthetic medical IoT traffic using machine learning, SN Comput. Sci. 5 (5) (2024) 1–15.
[50] K. Park, S. Noh, H. Lee, A.K. Das, M. Kim, Y. Park, M. Wazid, LAKS-NVT: Provably secure and lightweight authentication and key agreement scheme without verification table in medical internet of things, IEEE Access 8 (2020) 119387–119404.
[51] M.D. Rossetti, Simulation Modeling and Arena, John Wiley & Sons, 2015.
[52] A. Greasley, Simulation Modelling: Concepts, Tools and Practical Business Applications, Routledge, 2022.
[53] T. UcedaVelez, M.M. Morana, Risk Centric Threat Modeling: process for attack simulation and threat analysis, John Wiley & Sons, 2015.
[54] D. Gritzalis, G. Iseppi, A. Mylonas, V. Stavrou, Exiting the risk assessment maze: A meta-survey, ACM Comput. Surv. 51 (1) (2018) 1–30.
[55] M. Ekstedt, Z. Afzal, P. Mukherjee, S. Hacks, R. Lagerström, Yet another cybersecurity risk assessment framework, Int. J. Inf. Secur. 22 (6) (2023) 1713–1729.
[56] K. Kandasamy, S. Srinivas, K. Achuthan, V.P. Rangan, IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process, EURASIP J. Inf. Secur. 2020 (2020) 1–18.
[57] J.R. Nurse, S. Creese, D. De Roure, Security risk assessment in internet of things systems, IT Prof. 19 (5) (2017) 20–26.
[58] R.K. Yin, Case Study Research: Design and Methods, vol. 5, sage, 2009.
[59] Y. Sun, F.P.-W. Lo, B. Lo, Security and privacy for the internet of medical things enabled healthcare systems: A survey, IEEE Access 7 (2019) 183339–183355.
[60] A.I. Newaz, A.K. Sikder, M.A. Rahman, A.S. Uluagac, A survey on security and privacy issues in modern healthcare systems: Attacks and defenses, ACM Trans. Comput. Healthc. 2 (3) (2021) 1–44.
[61] A. Shostack, Threat Modeling: Designing for Security, John Wiley & Sons, 2014.

[62] I. Tarandach, M.J. Coles, Threat Modeling, O'Reilly Media, Inc., 2020.
[63] K. Wuyts, L. Sion, W. Joosen, LINDDUN GO: A lightweight approach to privacy threat modeling, in: 2020 IEEE European Symposium on Sec. and Privacy Workshops (EuroS&PW), IEEE, 2020, pp. 302–309.
[64] B. Schneier, Attack trees, Dr. Dobb's J. 24 (12) (1999) 21–29.
[65] V. Saini, Q. Duan, V. Paruchuri, Threat modeling using attack trees, J. Comput. Sci. Coll. 23 (4) (2008) 124–131.
[66] M.S. Lund, B. Solhaug, K. Stølen, Model-Driven Risk Analysis: The CORAS Approach, Springer Science & Business Media, 2010.
[67] W. Xiong, R. Lagerström, Threat modeling–a systematic literature review, Comput. Secur. 84 (2019) 53–69.
[68] A.A.A. Jilani, A. Nadeem, T.-h. Kim, E.-s. Cho, Formal representations of the data flow diagram: A survey, in: 2008 Advanced Software Engineering and Its Applications, IEEE, 2008, pp. 153–158.
[69] T.T. Allen, Introduction to Discrete Event Simulation and Agent-Based Modeling: Voting Systems, Health Care, Military, and Manufacturing, Springer Science & Business Media, 2011.
[70] V. Borodin, J. Bourtembourg, F. Hnaien, N. Labadie, COTS software integration for simulation optimization coupling: case of ARENA and CPLEX products, Int. J. Modelling Simul. 39 (3) (2019) 178–189.
[71] R.M. Czekster, R. Metere, C. Morisset, Incorporating cyber threat intelligence into complex cyber-physical systems: A STIX model for active buildings, Appl. Sci. 12 (10) (2022) 5005.
[72] R.M. Czekster, R. Metere, C. Morisset, cyberaCTIve: a STIX-based Tool for Cyber Threat Intelligence in Complex Models, 2022, arXiv preprint arXiv: 2204.03676.
[73] P. Empl, D. Schlette, D. Zupfer, G. Pernul, SOAR4IoT: securing IoT assets with digital twins, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022, pp. 1–10.