applied sciences

MDPI

Article

Challenges and Opportunities for Conducting Dynamic Risk Assessments in Medical IoT

Ricardo M. Czekster [1,*], Paul Grace [1], César Marcon [2], Fabiano Hessel [2] and Silvio C. Cazella [3]

[1] Department of Software Engineering and Cybersecurity, School of Computer Science and Digital Technologies, Aston University, Birmingham B4 7ET, UK; p.grace@aston.ac.uk

[2] Graduate Program in Computer Science (PPGCC), Polytechnic School, Pontifical Catholic University of Rio Grande do Sul (PUCRS), Porto Alegre 90619-900, Brazil; cesar.marcon@pucrs.br (C.M.); fabiano.hessel@pucrs.br (F.H.)

[3] Department of Exact and Applied Social Sciences, Federal University of Health Sciences of Porto Alegre (UFCSPA), Porto Alegre 90050-170, Brazil; silvioc@ufcspa.edu.br

* Correspondence: r.meloczekster@aston.ac.uk; Tel.: +44-(0)-121-204-4544

Abstract: Modern medical devices connected to public and private networks require additional layers of communication and management to effectively and securely treat remote patients. Wearable medical devices, for example, can detect position, movement, and vital signs; such data help improve the quality of care for patients, even when they are not close to a medical doctor or caregiver. In healthcare environments, these devices are called Medical Internet-of-Things (MIoT), which have security as a critical requirement. To protect users, traditional risk assessment (RA) methods can be periodically carried out to identify potential security risks. However, such methods are not suitable to manage sophisticated cyber-attacks happening in near real-time. That is the reason why dynamic RA (DRA) approaches are emerging to tackle the inherent risks to patients employing MIoT as wearable devices. This paper presents a systematic literature review of RA in MIoT that analyses the current trends and existing approaches in this field. From our review, we first observe the significant ways to mitigate the impact of unauthorised intrusions and protect end-users from the leakage of personal data and ensure uninterrupted device usage. Second, we identify the important research directions for DRA that must address the challenges posed by dynamic infrastructures and uncertain attack surfaces in order to better protect users and thwart cyber-attacks before they harm personal (e.g., patients' home) and institutional (e.g., hospital or health clinic) networks.

Keywords: dynamic risk assessment; cyber security; medical IoT; systematic literature review

check for updates

Citation: Czekster, R.M.; Grace, P.; Marcon, C.; Hessel, F.; Cazella, S.C. Challenges and Opportunities for Conducting Dynamic Risk Assessments in Medical IoT. *Appl. Sci.* **2023**, *13*, 7406. https://doi.org/10.3390/app13137406

Academic Editors: Dimitris Mourtzis and Stefano Silvestri

Received: 1 June 2023
Revised: 16 June 2023
Accepted: 20 June 2023
Published: 22 June 2023

1. Introduction

The latest advances in remote asset management have significantly changed the healthcare industry. Due to low costs and widespread adoption of the Internet-of-Things (IoT), wearable computing has enabled organisations to track and sense patients over secure telecommunication [1]. It is possible to attach devices to vulnerable patients under treatment and monitor essential physiological signs, such as cardiac rates, temperature, movement, and sugar levels, in near real-time [2]. Leveraging these IoT technologies away from hospital premises helps medical doctors make better and more timely decisions. This is due to the availability of important additional data that can then be analysed by automated information systems. Wearable devices can also empower patients to better understand and control their personal data sharing, thus preserving privacy objectives. However, these devices do pose a number of threats and vulnerabilities requiring attention and mitigative actions, and others have dubbed it the Internet of Threats [3].

In the healthcare domain, devices must adhere to additional constraints to ensure the safety and security of stakeholders. They must be compliant with other specifications and not interfere with underlying technologies. These devices are equipment referred to as Medical Internet-of-Things (MIoT), a subclass of IoT. MIoT sits within a broader cyber-physical system (CPS) [4] adding remote management capabilities over distributed assets [5–8]. Modern infrastructure design has incorporated MIoT into healthcare settings [9], especially after the COVID-19 pandemic [10]. Employing IoT in the patient's environment is highly advantageous; this typically involves IoT sensors monitoring patients and promptly transmitting data to sinks or servers for analysis. Solutions vary and examples include health prescription assistants (HPA), healthcare status monitoring (heartbeat, temperature, CO_2 levels, sensing features), tracking patients' movements, and detecting whether someone has fallen. Since its inception, security has been a key concern [11–13] and significant research has sought to address the security challenges and develop and deploy hardened solutions. All these inter-connected devices extend the feature set available to end-users; however, this comes with trade-offs between privacy and cyber security objectives. Despite having to comply with regulations by vendors, they must be sufficiently equipped with mechanisms to cope with accidental and deliberate malfunctions. These failures could be caused by flawed designs, poor testing, or active cyber-attacks aiming to exfiltrate personal and identifiable information (PII) [14] from stakeholders. Governments and organisations are enforcing legislation to protect users and patients, for instance, the Health Insurance Portability and Accountability Act (HIPAA), in the US, and the General Data Protection Regulation (GDPR), in the UK and European Union (EU). These efforts signal the need to safeguard and protect data with clear repercussions for violations; this further highlights the importance of secure MIoT systems.

Stakeholders employing these technologies are under constant risk (for different meanings of 'risk', please refer to Appendix A.1) arising from different threat sources with varied impacts and occurrence likelihoods. Asset managers sitting on the edge of the infrastructure desire to offer end-users, customers or patients hardened MIoT equipment with protective assurances to ensure seamless interactions. They employ embedded software communicating status and health-related data that feed information systems (IS) so medical doctors can make timely choices to improve care delivery. These platforms, albeit tested widely by vendors before shipping, are not immune to the malicious advances of sophisticated threat actors. One remedy for establishing protections is to perform risk assessment (RA), choosing a methodology [15] with specific considerations for medical-based IoT [16]. Alternatives are the ISO 31000:2018 standard [17], NIST 800-30r1 [18], operationally critical threat, asset, and vulnerability evaluation (OCTAVE) and OCTAVE Allegro [19], as well as a plethora of RAs available for risk managers [20].

While RA is a proven method in identifying and mitigating security risks, it is traditionally only performed periodically. In highly dynamic systems, the important factor is change. This is especially true of IoT, where the system or the environment may change (changing the attack surface). For example, new sensors can be deployed, or devices may switch to a new network. Furthermore, new attacks will emerge. Periodic RA is unable to respond to these changes and ensure risk is managed in a timely fashion. Zio (2018) [21] has discussed the future of RA, establishing the most relevant aspects to incorporate dynamic elements directly into the analysis. This RA variant called dynamic risk assessment (DRA) targets continuous, near real-time, on-the-fly reassessments. Applying DRA in IoT is not new, as it has been addressed in many discussions [22,23] and case studies for threat-based RA in smart homes [24–27]. These studies highlight that DRA provides better observability (this term comes from control theory and distributed systems [28]; it is used nowadays as a means to understand a system's states by inspecting the data it generates in event logs, metrics, etc. to append protective features) features to systems when tackling unknowns situations [29], i.e., events that "we do not know we do not know" [30].

The driving motivation here is the fact that, where MIoT systems are deployed and utilised, there is a dynamic attack surface. While existing risk assessment methods have proven successful in traditional systems, the dynamic nature of this environment requires RA to be revisited and led to the consideration of dynamic RA. There have been few research/studies into this and, hence, this review and its observations are important, timely and novel. The motivation described has been explicitly introduced in the introduction.

Thus, this work discusses the inherent challenges of conducting DRA in MIoT to enumerate effective ways of tackling *emergent risks* to patients through wearable computing in healthcare. The paper makes three key contributions:

- A comprehensive systematic literature review (SLR) of risk analysis and its application to MIoT; this highlights the current trends and existing approaches in this domain.
- An exploration of effective strategies for mitigating the impact of unauthorised intrusions and safeguarding end-users against the leakage of PII or the disruption of equipment usage in dynamic MIoT systems.
- The identification of the key research directions for DRA that must address the challenges posed by dynamic MIoT infrastructures and uncertain attack surfaces in order to better protect users and thwart cyber-attacks.

We focus on malicious opportunities that sophisticated threat actors may explore in MIoT. Our investigation outlines the most common risk approaches in large attack surfaces and the issues behind using DRA when coping with service and system interruptions.

The paper is organised as follows: Section 2 outlines the context for MIoT and Section 3 explores related work and our SLR. This is continued in Section 4, which details the challenges and opportunities behind tackling RA and DRA in IoT. We end our contribution in Section 5 with conclusions and discussion of future work.

2. Contextualisation

2.1. Threat Modelling, Static and Dynamic Risk Analysis

Recent years have witnessed the ever-increasing adoption of IoT-based devices in a myriad of application contexts [31]. Examples are Industrial IoT (IIoT), smart manufacturing, smart cities [32,33], energy generation/storage, and healthcare domains [34]. Although these devices offer remote management capabilities and near real-time sensing, when considering cyber security and privacy, they have considerably enlarged the potential attack surface to protect [35]. Integrating RA and threat modelling (TM) is a traditional information security approach to protect such distributed assets. A noteworthy approach is the process for attack simulation and threat analysis (PASTA), a risk-oriented TM framework that assumes security practitioners are risk managers [36]. It is targeted at helping organisations tackle inherent risks in software to devise hardened products to sustain response to cyber-attacks. Wolf et al. (2021) [37] applied the approach to IoT ecosystems showcasing its use with DFDs to demonstrate trust boundaries, as well as presenting an abuse-case diagram for a light control system.

According to the ISO [17], tackling risk is about determining *uncertainty*, whereas for NIST/US [18], it is a holistic approach encompassing organisations, business processes and information systems. DRA is a relatively recent approach to handle change and assess risk continuously, i.e., to update the RA as new evidence (data) emerges in networks and feeds, proactively preparing for malicious incursions as they progress [23,38,39]. As previous work has discussed in detail in the recent literature [40,41], conducting such analysis in IoT is not trivial, a theme we shall cover in Section 4.

TM is an exercise in assessing opportunities for system abuse by threat actors and creating the means to cope, withstand or mitigate existing vulnerabilities [42–44]. Threat analysts could perform TM in the early stages and continuously as managers and system administrators incorporate new technologies and devices into the solution. TM has been successfully used in healthcare [45] to promote better countermeasures and mitigations to specific attacks inherent in IoT shortcomings [46]. Among many techniques available to analysts, we highlight attack trees/graphs and data-flow diagrams (DFD) [47] to depict such concerning situations and employ TM to understand how to address and mitigate governing issues, among other approaches.

Regarding specific RA frameworks tailored to MIoT, we highlight the IoMT security assessment framework (IoMT-SAF) [48]. It involves healthcare stakeholders in risk processes, allowing them to assess the level of security as observed in distributed MIoT devices across the attack surface. The framework identifies security issues, recommends responses and creates scenarios for stakeholders using an ontological approach. The IoMT-SAF's process encompasses identifying security properties, such as: (i) medical operation security; (ii) vulnerability type (user, system, hardware); (iii) attack origin (local, remote), attack type (passive, active), attack difficulty (theoretical, difficult, easy, tools available); (iv) security function (detection, prevention, incident response); and (v) medical data threat (interception, interruption, modification, fabrication, replication).

2.2. Medical IoT

Working with IoT technologies in healthcare, there are a myriad of similar notions and definitions that we differentiate next. For instance, we have encountered references to the Health Internet of Things (HIoT) [49], the Internet of Health Things (IoHT) [50,51], the IoT-Health [52], the Internet of Medical Things (IoMT) [53–55], and the Medical Internet of Things (MIoT) [1,2,56]. In this work, we shall refer to the latter (MIoT) as a base definition as we think it captures the fundamental differences between general IoT systems versus those applied to medical/healthcare contexts with its more specific subtleties. MIoT empowers patients and clinical staff (in general) to understand care paths and plan interventions. It allows tracking, sensing and near real-time screening of patients that alert responsible personnel in case they detect or observe any anomaly using tailored algorithms that are either running on devices or using auxiliary information systems.

Understanding risk in systems is typically founded upon understanding the system itself. Evaluating a system architecture is, therefore, a starting point. Within IoT systems, the architecture has most simply been considered as a basic three-layer approach, composed of the *perception layer*, the *network layer* and the *application layer* [57]. While it is beyond the scope of this work to assess what is the best architecture to underpin security and privacy risk assessment, we note that these basic models constrain the system viewpoints potentially missing key IoT vulnerabilities. Hence, architecture model extensions, such as a *middleware layer*, a *business layer*, an *end-user layer*, a *processing layer* and a *service management layer* [58–60] could offer a better perspective. Security analysts overseeing large dynamic attack surfaces may then consider threat actors attempting to circumvent controls and exploit vulnerabilities on each layer as they have specific protocols and inter-layer dynamics [61,62]. Farahani et al. (2018) [63] go beyond this notion and consider different scales of *IoT layers*, dividing these into three types—wearables, smart homes and smart cities—across four layers: interface, service, networking and sensing.

2.3. MIoT Security and Privacy

Recently, NIST/US published a draft version for Trusted IoT Device Network-Layer Onboarding and Lifecycle Management (NIST SP 1800-36) [64], showcasing how to tackle credentials to connect to networks securely (Link to NIST/US site: https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management, accessed on 19 June 2023).

One assumes that this document would be used alongside NIST's cybersecurity framework (NIST SP 800-37) (NIST Cybersecurity Framework: https://www.nist.gov/cyberframework, accessed on 19 June 2023), a guide to help organisations seeking to improve cyber security risk management. In the same direction, the UK's National Cyber Security Centre (NCSC) publishes risk management guidance (NCSC Risk Management Guidance: https://www.ncsc.gov.uk/collection/risk-management-collection, accessed on 19 June 2023), and the European Union Agency for Cybersecurity (ENISA/EU) has tackled risk management and assessment, providing tools and interoperability discussions among the many frameworks available to organisations (ENISA Risk Management and RA Framework: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/business-process-integration/the-enisa-rm-ra-framework, accessed on 19 June 2023).

Elhoseny et al. (2021) [57] suggested that MIoT has stricter security and privacy requirements in contrast to 'usual' IoT. The complex MIoT ecosystem presents a massive attack surface requiring constant monitoring, confidential communication among trusted parties, data integrity, resilience to attacks, auditing (for backtraces or forensics), access control, authentication, and privacy [16]. For healthcare settings located at home, these assurances must hold, preventing attacks, avoiding exposure, and thwarting attacks before they cascade to adjacent networks and systems. It is outside the scope of this work to list and comment on specific cyber-attacks on MIoT as there has been a host of research explaining these over the years [15,27,35,62].

Complementing the MIoT ecosystem with cyber security counterparts, one could add the usual protections, i.e., intrusion detection systems (IDS), firewalls (and filtering scripts), encryption and access control (and varieties such as rule-based and attribute-based) as well as privacy-enhancing technologies , such as private information retrieval (PIR), virtual private networks (VPNs), transport layer security (TLS), combined with domain name system (DNS) SECurity extensions (DNSSEC). Nowadays, in the areas of IoT and trust mechanisms, there have been discussions on incorporating distributed ledger technologies (DLT) [65] or *blockchains* to enact effective *chains of trust* among multiple counterparts, objects and services in a decentralised manner [66–68]. Yadav et al. (2023) [69] have employed blockchain-based technologies in IoT to enable secure and reliable communications in smart cities. There are efforts to improve the scalability, resilience and trust mechanisms offered by DLT through a technology called IoT application (IOTA) [70–73], a next-generation blockchain solution.

Other noteworthy concepts associated with healthcare, and which use technologies to sustain additional communication and remote management features, include employing patient health information (PHI) and storing it under electronic health records (EHR). Some authors have also included so-called healthcare systems, such as electronic medical recording (EMR), order communication systems (OCS), and picture archiving and communication systems (PACS) [41]. These systems must comply with underlying cyber security IS, such as IDS, firewall/filtering, security information and event management (SIEM), and continuous cyber security monitoring and logging practices [74].

IoT and MIoT are targets for a host of cyber-attacks [35,62,75]. As Alsubaei et al. (2019) [48] commented, approximately 45% of all ransomware attacks dating 2017 were directed at the healthcare sector. In 2018, cybercriminals deployed WannaCry ransomware and Zero-day attacks in healthcare facilities in the UK's National Health Service (NHS), encrypting all data in unpatched systems [76,77]. Stellios et al. (2018) [75] discussed IoT security and TM in detail, highlighting attack venues explored by threat actors. For instance, they highlighted issues such as DoS, physical threats, eavesdropping, node capture and compromisation. Their work focused on modelling IoT-enabled cyber-attacks by understanding: (i) adversaries (access, motivations, capabilities); (ii) IoT devices (embedded system vulnerabilities, network vulnerabilities); and (iii) actual targets connectivity (direct, indirect, no connection to critical infrastructure).

3. Systematic Literature Review

We conducted an SLR to better understand how researchers consider risk assessment in MIoT/IoT. It employed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 recommendations [78], following the 27-point checklist for deriving a substantial synthesis of research priorities, where we use the relevant items as dictated by the PRISMA process. We provide below a summary of the PRISMA 2020 Checklist (referring to items from the recommendations as #) with regard to the 'Introduction' and 'Methods':

- Rationale (#3)—the literature about risks in MIoT must be better understood. In past years there has been a proliferation of research that would profit from synthesis and discussion to organise knowledge and identify gaps.
- Objectives (#4)—the guiding question is *"What are the factors underpinning risk assessments in MIoT?"*.
- Eligibility criteria (#5)—as inclusion criteria, we are interested in the latest results (published in the last five years, i.e., May 2018 to May 2023) mentioning risk assessment (any type, i.e., normal, i.e., in this context, we refer to the *usual* way organisations

conduct RA, by following guidelines and deriving the most likely risk scenarios that could arise, vulnerabilities, impact and mitigation effort that follows—or dynamic, describing case studies in healthcare that used MIoT for data gathering and communication). Our exclusion criteria do not consider any poster not providing fundamental research outcomes, results not focused on cyber security or privacy, as well as RA that does not consider the use of IoT/MIoT.

- Information sources (#6)—Google Scholar, ACM Digital Library and IEEExplore (Respectively, https://scholar.google.com, accessed on 19 June 2023, https://dl.acm.org, accessed on 19 June 2023, and https://ieeexplore.ieee.org, accessed on 19 June 2023).
- Search strategy (#7)—our basic template for input was:
  - Query: `(dynamic risk assessment or risk assessment) and (“medical IoT” or MIoT) and healthcare and (cybersecurity or “cyber security” or cyber-security).`

  We adapted it to match the particularities of the information source under scrutiny.
- Selection process (#8)—case studies employing risk assessment of MIoT/IoT in healthcare settings.
- Data collection process (#9)—we performed the search, analysed titles and abstracts and then retrieved the entire paper for in-depth inspection as to eligibility.
- Data items (#10)—for the selected papers that passed previous stages of scrutiny, we extracted RA methodology and relevant risk-related components, healthcare settings (if any), MIoT/IoT specification (if any), year and case study explanation. Depending on the selected research, we were interested in any cyber-attack or specific vulnerability comprising MIoT/IoT devices.

Our guiding search strategy was directed at RA approaches that were either static/periodic or dynamic. We also investigated the security issues that the technologies try to solve or tackle, i.e., blockchains used for trust parties, lightweight authentication, or fast encryption for confidential data manipulation. In addition, we addressed the most likely types of cyber-attacks that threat actors could attempt when abusing systems.

We tweaked the searching input query to match the specific requirements of the information sources—for instance, using parentheses is mandatory to convey precise relationships. For Google Scholar, we executed the template query explained above and then selected the “Custom Range” parameter to retrieve papers sorted by relevance from 2017 to 2022. As this platform does not only scan scientific venues per se, we were interested in all retrieved gray literature, such as dissertations, manuals, and white papers.

Specifically for ACM-DL, the mechanism required logical connectors all to be uppercase. The query was:

```
[[Full Text: dynamic risk assessment] OR [Full Text: risk assessment]] AND
[[Full Text: ‘‘medical iot’’] OR [Full Text: miot]] AND
[[Full Text: cybersecurity] OR [Full Text: ‘‘cyber security’’] OR
[Full Text: cyber-security]] AND
[E-Publication Date: (01/01/2017 TO 31/12/2022)]
```

For IEEExplore, the same query used in Scholar and ACM-DL yielded zero results, prompting us to edit the *Advanced Query* option to *build* the query as the platform expected. Then, for this source, we had to edit the query manually, so it applied the logical connectors with parentheses following this query filtered out by year (2017 to 2022):

```
((‘‘All Metadata’’: ‘‘dynamic risk assessment’’
OR ‘‘risk assessment’’) AND
(‘‘All Metadata’’: ‘‘medical iot’’
OR ‘‘miot’’ OR ‘‘iot’’) AND
(‘‘All Metadata’’: ‘‘cybersecurity’’
OR ‘‘cyber security’’
OR ‘‘cyber-security’’))
```

3.1. Related Work on RA/DRA in MIoT

We conducted the SLR between 2 May 2023 and 6 May 2023 for all the chosen information sources. Figure 1 shows the suggested PRISMA 2020 flow diagram for SLR, which includes searches of databases.

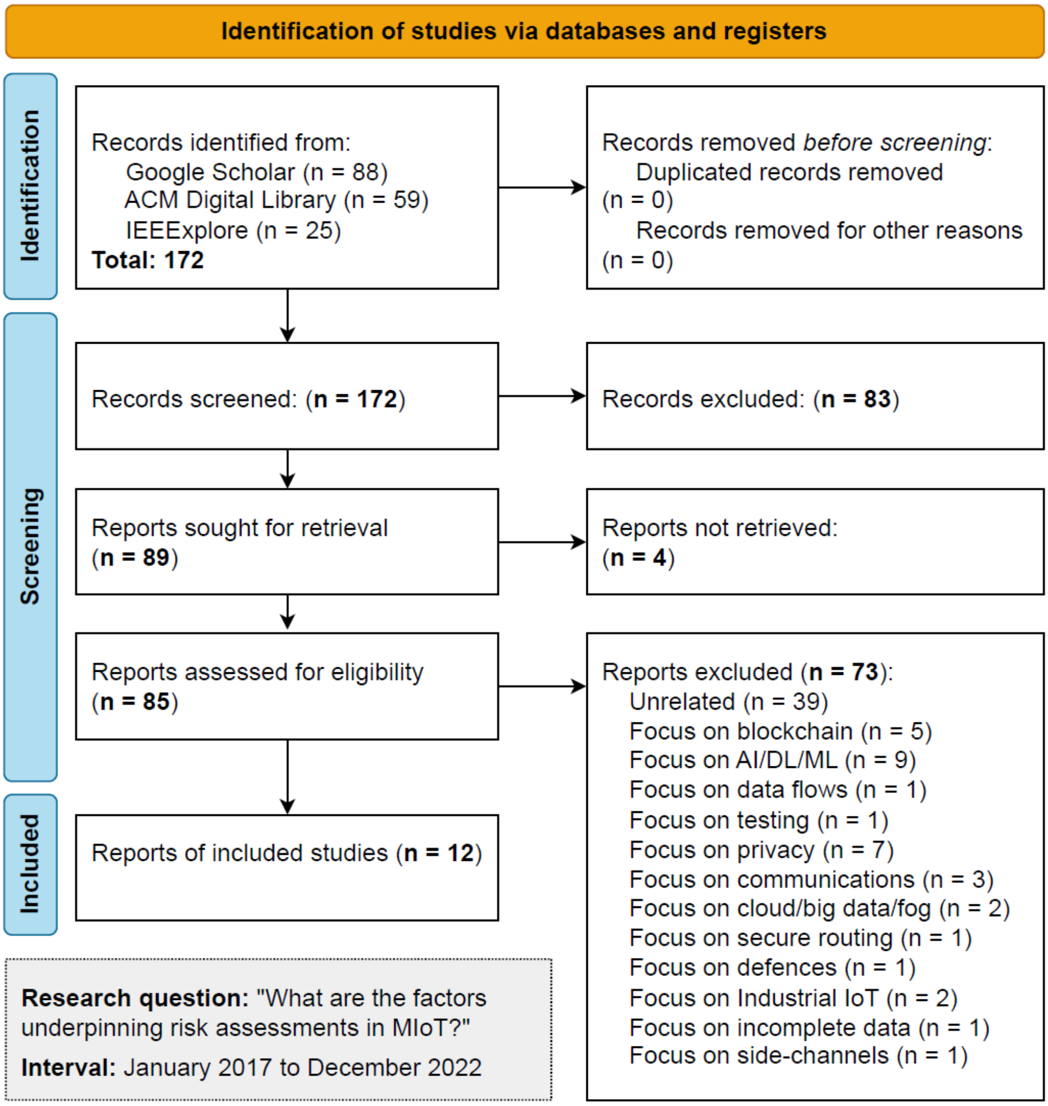
Identification of studies via databases and registers
Identification
Screening
Included
Records identified from:
Google Scholar (n = 88)
ACM Digital Library (n = 59)
IEEExplore (n = 25)
Total: 172
Records removed *before screening*:
Duplicated records removed (n = 0)
Records removed for other reasons (n = 0)
Records screened: (**n = 172**)
Records excluded: (**n = 83**)
Reports sought for retrieval (**n = 89**)
Reports not retrieved: (**n = 4**)
Reports assessed for eligibility (**n = 85**)
Reports excluded (**n = 73**):
Unrelated (n = 39)
Focus on blockchain (n = 5)
Focus on AI/DL/ML (n = 9)
Focus on data flows (n = 1)
Focus on testing (n = 1)
Focus on privacy (n = 7)
Focus on communications (n = 3)
Focus on cloud/big data/fog (n = 2)
Focus on secure routing (n = 1)
Focus on defences (n = 1)
Focus on Industrial IoT (n = 2)
Focus on incomplete data (n = 1)
Focus on side-channels (n = 1)
Reports of included studies (**n = 12**)
Research question: "What are the factors underpinning risk assessments in MIoT?"
Interval: January 2017 to December 2022

Figure 1. PRISMA 2020 identification of studies.

Regarding the process, the initial identification resulted in 172 records, with four removed for being duplicates or unavailable. The next phase screened these records and excluded 83 because the title or abstract was unrelated to our SLR proposition. We assessed 85 reports, reading all the work and excluding 73 for various reasons related to not meeting the previously identified eligibility criteria. The process finished with selecting 12 studies, where we extracted significant risk-associated elements, frameworks, standards, attacks, and methodologies to support our discussion. Table 1 summarises the main findings from the SLR, presenting an overview of selected work on RA/DRA. Note that some literature is specific to MIoT, and some discusses IoT in broader terms.

Le et al. (2018) [79] devised a DRA framework in the context of autonomous vehicles. This work did not make it into the SLR because it was not applied to healthcare; however, it includes important discussions and observations for proposing a dynamic framework for tackling risk. The authors comment on the requirements and challenges for developing a DRA framework in highly dynamic environments with frequent threats, vulnerabilities and technological changes. They justified the need for such an approach because systems should quickly adapt to unstable environments from various IoT sources. As stated, the risk framework should:

1. Deal with heterogeneous data.
2. Eliminate inconsistency and incompleteness, managing uncertainty errors and missing values, increasing data *reliability*.
3. Reduce the data scale for efficient processing.
4. Provide run-time risk analysis for effective and actionable decision making.

Table 1. Overview of selected literature on RA/DRA in IoT/MIoT.

#	Authors	Domain	Highlights
#01	Kandasamy et al. (2020) [80]	IoT, MIoT	Showcases RA frameworks in IoT, computes MIoT risk, IoT risk vectors and risk ranking
#02	Lee (2020) [58]	IoT	Proposition of a four-layer IoT cyber risk management framework, risk identification, quantification
#03	Ksibi et al. (2021) [81]	MIoT	Dynamic agent-based risk management, generic case studies in IoT/MIoT, enhance trustworthiness of MIoT
#04	Malamas et al. (2021) [16]	MIoT	SLR, discussing risk assessment frameworks in MIoT, comments on "medical risk" and risk methods
#05	Stellios et al. (2018) [75]	IoT, MIoT	Methodology uses attack model to output qualitative criticality level of IoT-enabled devices
#06	Elhoseny et al. (2021) [57]	MIoT	Focus on security and privacy of MIoT, CIA, resilience, access control, usability, data issues
#07	Kandasamy et al. (2022) [82]	IoT	Risk assessment focused on NIST Cyber Security Framework using self-assessment survey instruments
#08	Newaz et al. (2021) [83]	IoT	Discusses the benefits of fault-tolerant designs to improve security, a survey of known attacks in IoT
#09	Gressl et al. (2020) [84]	IoT	Use of known methods to address risk, e.g., design space exp. (DSE), Bayesian attack graphs, risk trees
#10	Datta (2020) [23]	IoT	Combination of risk assessment framework with security incident and event management altogether
#11	Nurse et al. (2017) [40]	IoT	Describes core RA concepts in IoT, Comments on deficiencies of RA approaches and their inadequacy
#12	Nurse et al. (2018) [41]	IoT	Discusses the need for automated and collaborative RA in IoT, with industrial comments and practices

3.2. Analysis of Selected Results

We next comment the selected papers and conduct an in-depth analysis outlining the major strengths and relevant considerations for tackling risks in IoT/MIoT ecosystems. The number of included studies is low because, after executing all of the PRISMA procedure, it favours quality over quantity, i.e., we will retrieve and scrutinise only the most relevant results aligned with the SLR's research question.

#01 by Kandasamy et al. (2020) [80] comments on IoT-based vulnerabilities, such as complex architecture, inappropriate security configuration, physical security, and insecure firmware or software; it discusses how to address computation of cyber-risk referring to risk ranking, risk vectors, and risk assessment frameworks. The work tackles known impact factors, likelihood, and risk levels in IoT and comments on the risk assessment process (RAP) of known standards, such as NIST, ISO/IEC, OCTAVE, GSMA (It is called the Self Assessment Risk Management Toolkit, link: https://www.gsma.com/mobilefordevelopment/resources/self-assessment-risk-management-toolkit-summary/, accessed on 19 June 2023) (based on OCTAVE), and threat assessment and remediation analysis (TARA). It compares various RA frameworks specifically for IoT, computing the MIoT risk for medical devices and discussing RA scales and rankings. It comments on known IoT risk vectors and risk rank calculation, devising numerical weights for computing risk likelihood parameters.

#02 by Lee (2020) [58] discusses qualitative, e.g., ISO, cyber kill chain (CKC), OCTAVE, capability maturity model integration (CMMI), and consensus audit guidelines (CAG), as well as quantitative approaches, namely, Bayesian decision network (BDN), AVARCIBER, an extension of ISO 27005, and NIST's approach geared towards cyber security risk management. The four-layer risk management framework comprises the following: (i) an IoT cyber ecosystem layer; (ii) an IoT cyber infrastructure layer; (iii) an IoT cyber risk assessment layer; and (iv) an IoT cyber performance layer. It identifies risk by inspecting IoT assets, vulnerabilities and cyber threats and quantifying risk by looking at each IoT asset's impact, frequency, and defence probability in terms of vulnerabilities and classifying it into different cyber threat groupings. It allocates IoT resources in a financial/budget scheme for cost-benefit analysis with mechanisms to break down IoT-based layers in a divide-and-conquer risk approach.

#03 by Ksibi et al. (2021) [81] proposes a risk management framework relying on an orchestrator and three agents for managing risks in the device, network and storage and processing areas. It focuses on RA, specifically e-health that employs haemodialysis and cardiac devices. The objective is to simplify the complexity of cyber-risk management efforts and to establish a fine-grained risk management process. The main idea is to evaluate the cumulative risk associated with global e-health service and to automate response for risk mitigation. It proposes dynamic agent-based risk management with risk identification, analysis/evaluation, and adaptation, followed by classification and risk evaluation, encompassing risk impact/cost, anomaly probability, global risk evaluation, and model evaluation. The framework is generic to IoT/MIoT, and it aims to study security challenges in e-health networks, enhancing trustworthiness in MIoT communicating nodes for decision-making on a layered risk management model.

#04 by Malamas et al. (2021) [16] provides a comprehensive comparison among RA methodologies and TM applied to MIoT, e.g., ISO, NIST, EU Regulation 2017/745 for Medical Devices, Open Worldwide Application Security Project (OWASP) IoT vulnerabilities, MAYO Clinic, ENISA, Association for the Advancement of Medical Instrumentation (AAMI), Australia's Therapeutic Goods Administration (TGA), and MITRE/US. For TM, they cover spoofing, tampering, repudiation, information disclosure, denial-of-service, elevation of privilege (STRIDE), damage, reproducibility, exploitability, affected users, discoverability (DREAD), attack trees, and multiple-valued logic (MVL). The authors propose a generic risk model for MIoT inspired by NIST's terminology (e.g., predisposing conditions and adverse impact). This generic model invites security analysts to conduct thorough security assessments for threat, vulnerability, and impact assessment, risk mitigation or risk treatment. The work suggests that traditional RA methodologies cannot be applied to MIoT contexts because they belong to untrustworthy environments where the designer favours end-customer usability over security.

#05 by Stellios et al. (2018) [75] focuses on 'verified attacks', i.e., real-world incidents or attacks published by researchers with applications on IIoT, e-health IoT and smart systems. The authors explain attacks in depth as applied to critical infrastructure, which encompasses smart infrastructure and healthcare, among others. The work details an e-health medical IoT system for two ecosystems, comprising *in-hospital* and *near-patient*. Consistent with the direction of our work, the authors suggest that security attacks targeted explicitly at CPS and IoT have been addressed throughout the years; however, they have only sometimes been fully assessed and understood.

#06 by Elhoseny et al. (2021) [57] compartmentalises IoT provisions and attacks perpetrated on each layer, detailing protections and protocols. The authors also comment on available countermeasures, e.g., access control, data encryption, data auditing, IoT healthcare policies, data search, data minimisation and anonymisation, inventory devices, network segmentation, following the security community's best practices, awareness, and continuous monitoring and reporting. There is a focus on the security and privacy requirements of MIoT, such as confidentiality, data integrity and availability, resilience to attacks, data usability, access control, data auditing/authentication, and privacy of patient information. The work details the MIoT infrastructure comprised of wireless body area networks (WBAN), sensing, cloud, and medical staff, all contributing towards effective patient care. They describe real-time location services (RTL) for IoT devices for tracking employees, patients, visitors, and assets. Finally, they comment on the need to perform regular RA to identify potential risks associated with MIoT. This should be set up and designed to understand vulnerabilities better before the environment becomes operational.

#07 by Kandasamy et al. (2022) [82] focuses on the NIST cyber security framework combined with self-assessment survey instruments for understanding vulnerability and risk. The work refers to vulnerability and threat pairs that produce two other risk indices, risk management culture (RMC) and risk process and technology (RPT), applied to Asia-based healthcare cyber-attacks. The objective was to understand cyber security maturity from a vulnerability and risk perspective in order to compute a so-called enriched vulnerability priority score (EVPS) to prioritise vulnerabilities for managers to consider for counteracting attacks.

#08 by Newaz et al. (2021) [83] considers medical standards for cyber security ((IEC 62304:2006, ISO/IEC 27032:2012, IEC 82304-1:2016, ISO/IEC 8001 (Risk Management of Medical Devices on a Network), IEC/TR 80002-1:2009, ISO/TR 800020-2:20017, IEC/TR 80002- 3:2014). The authors comment on fault-tolerant designs to harden the infrastructure. The work comprises a survey that provides good explanations and classification of medical concerns employing IoT/IoMT. For instance, the authors suggest the following classification: *non-invasive* devices, *invasive* devices (transient use, short-term, long-term and connected), and *active therapeutic* devices (e.g., muscle stimulators and hearing aids). They offer a classification of sensors in terms of *physiological* (measure ECG, electromyography), *biological* (glucose, alcohol), and *environmental* sensors (accelerometer and gyroscope in smartwatches). In terms of cyber security protections, the work suggests using intrusion detection mechanisms to infer and confirm attacks, fine-grained access controls, privacy-preserving healthcare systems, employing artificial intelligence and machine learning (AI/ML) and big data, and in-depth investigation of smart medical devices and existing threats.

#09 by Gressl et al. (2020) [84] presents and explains design space exploration (DSE), Bayesian attack graphs (BAG), and risk trees (RISKEE). The authors provide a design framework to study a system's attack susceptibility to model security constraints. They comment on the need to incorporate RA in early system design and the advantages of drawing upon these choices. The paper showcases examples of limited capacity infrastructure, where they compute attack probabilities and the mean risk value for the setting under study.

#10 by Datta (2020) [23] presents three critical elements for performing thorough RA: (i) cyber security risk assessment framework; (ii) security incident and event management; and (iii) resilience framework. It extends the European Telecommunications Standards Institute (ETSI) risk-based security assessment. It showcases the framework using the following steps: (i) understanding business cases and regulatory contexts; (ii) business processes identification and security requirements; (iii) risk identification, estimation, evaluation and security testing; (iv) assets—cloud web services, IoT devices and networks;

and (v) upgrading software modules of end-to-end IoT platforms. This work brings together a risk assessment framework and an SIEM system as a significant contribution.

#11 by Nurse et al. (2017) [40] describes *core RA concepts*, as generally understood, as the process of identifying, estimating and prioritising risks to comprise organisational assets and fulfil operations. It comments on the usual approaches for RA, namely, NIST SP 800-30, ISO/IEC 27001, OCTAVE, the Central Communication and Telecommunication Agency (CCTA) Risk Analysis and Management Method (CRAMM), and *Expression des Besoins et Identification des Objectifs de Sécurité* (EBIOS) (ENISA's link: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html, accessed on 19 June 2023). It discusses particularities related to IoT dynamics including: (i) variability of scale in devices and systems; (ii) dynamism and temporality of connections between devices; and (iii) heterogeneity of actors interacting with IoT ecosystems. The authors provide substantial discussions to consider *"where current risk assessment methods fail?"*. They argue that it is mainly a result of lack of periodic assessment triggered by unobserved changes in the system (attack surface), business processes, or new information arising from threat intelligence mechanisms in place. The authors outline why current RA approaches are inherently inadequate when tackling IoT, providing interesting discussions. As a remedy, they advocate automated and continuous RA and the development of supporting tools to assist in simulation and modelling to enhance prediction and enable better preparedness.

#12 by Nurse et al. (2018) [41] refers to the IoTRiskAnalyzer framework [85], probabilistic model checking, Bayesian techniques combined with attack graphs and inference networks, and SecKit as a valid approach to provide model-based security and to address IoT-related risks. The authors discuss the need for automated RA in the IoT and collaborative risk assessment practices to enhance timely analysis. In the discussions provided, they refer to the *"perceived infeasibility of fully automated risk assessment in the IoT, and a view towards inter-organisational assessment of risk given IoT's wide connectivity"*. This factor is based upon the opinions of cyber security professionals taking part in the user study, as opposed to any experimental work showing what is/is not technically possible. The work describes an exciting set of industrial practices, including with fruitful discussions relating to concerns and observations about the difficulties of tackling timely RA in IoT.

After closely inspecting these results, some themes emerged. For instance, authors often remarked on the need to engage in layered approaches when tackling risk in IoT/MIoT networks [58,81]. Understanding the types of devices (invasive, non-invasive), as well as the types of sensors (physiological, biological, environmental), could also help understand underlying protections to adopt [83]. There are also comments on risk quantification as referred to in a significant number of studies [80–82]. The need for understanding how organisational culture could address cyber security and withstand or mitigate cyber-attacks as they progress as well as maturity-related concerns was also highlighted [82]. There were also comments on the requirement for continuous RA and collaborative RA to enact timely protections for stakeholders [40,41] and relating to response automation [81].

Next, we provide an overview of interesting ideas and concepts extracted from our in-depth results analysis:

- Risk-related standards (for a list of standards, please refer to Appendix A.3)—ISO 27000, IEC 62304:2006, ISO/IEC 27032:2012, IEC 82304-1:2016, ISO/IEC 8001 (Risk Management of Medical Devices on a Network), IEC/TR 80002-1:2009, ISO/TR 800020-2:2017, IEC/TR 80002-3:2014, ETSI's risk-based security assessment, CCTA CRAMM, EBIOS.
- Organisations—MITRE/US, AAMI, TGA, EU regulations, ENISA, OWASP, ETSI.
- Other standards—CMMI, CAG.
- RA methodologies—ISO 27000, NIST 800-30, OCTAVE and OCTAVE Allegro.
- Other methodologies applied to risk—IoTRiskAnalyzer, SecKit, attack graphs.
- Threat modelling and techniques—STRIDE, DREAD, TARA, attack/risk trees, MVL, CKC, BDN, DSE.

- Catalogues of vulnerabilities—OWASP Top 10 IoT vulnerabilities.
- IoT services and features—security (CIA attributes, as explained in Section 4) and safety; device and system interoperability; resilience to attacks and fault-tolerant design; authorisation, authentication, access control; use of real-time location services (RTL) for tracking employees, patients, visitors, and assets; accounting for dynamism and temporality of devices in dynamic settings.
- Risk quantification—likelihood, impact, and vulnerability prioritisation.
- IoT ecosystems—in-hospital (within a hospital's premises) and near-patient (within patients, wherever they are located, e.g., at home or in other settings).
- IoT layers—basic representations encompass three layers, namely, perception, network, and application; however, as previously mentioned, the literature considers extensions such as middleware, business, end-user, processing, and service management, which can drive assessment efforts as each layer presents its own set of weaknesses that sophisticated threat actors can potentially exploit.

From a patient's perspective, their smart-based apparatuses may interfere with their medical equipment. For instance, Pal et al. (2018) [86] studied IoT in smart homes and the future prevalence of ambient assisted living (AAL) technologies to revolutionise remote care and treatments for the elderly. The benefits of such technologies should meet stringent security requirements, but offer a balance in terms of respecting privacy whilst monitoring patients. One cannot dismiss the fact that these novel smart home setups are not immune to cyber-attacks as sophisticated actors may deploy malware or eavesdrop on communications for financial gain or for other motives.

4. Challenges in Performing Risk Assessment in MIoT

Cyber security generally entails addressing attributes such as confidentiality, integrity, and availability, known as the CIA triad [87,88]. Over the years, some authors have started to define these attributes in terms of related characteristics, such as authorisation, authentication, non-repudiation, auditing and accountability; however, these are almost synonyms to the terms used by CIA. Any attack directed at a system attempts to disrupt one of these attributes, so security officers enact protections to assets by designing robust systems that may withstand malicious incursions and stop attack progression before affecting other systems. The methodology we follow next consists of identifying relevant literature on RA and DRA, mapping concerns and challenges, and discussing significant shortcomings and difficulties whilst addressing risks in IoT/MIoT.

Nowadays, organisations hire proficient cyber security personnel to guide protective actions and comply with regulations to protect customers. Failure to do so can be caused by poor preparedness, lack of specific training in cyber security (unskilled staff), situational awareness deficiencies in understanding and mapping the attack surface (poor asset visibility), and unfocused security monitoring, among other factors. Hiring proficient cyber security personnel with a background in mitigation, responses, and with pro-active cyber security skills certainly helps organisations cope with impending attacks and to thwart malicious occurrences, and to differentiate between localised anomalies caused by incompetent configurations or improper device use [89,90].

Other vital cyber security research [91] addresses the (i) sheer scale of cyberspace, where potentially billions of interconnected devices interact, and the (ii) asymmetry between attack and defence, where threat actors only need to identify a single point of attack, while defenders seek to prevent or block any vulnerabilities in their systems and services. Another recurrent issue is related to the poor design and implementation of software or firmware that permeates the industry and insufficient testing that allows vulnerable products and services to reach end-customers [11,92].

Risk in medical devices has been addressed in early literature dating back to 2007 [93] under the ANSI/AAMI/ISO 14971:2007 standard (please refer to Appendix A.2 for the definition), which suggests that risk has two components: (i) the probability of occurrence of harm; and (ii) how severe that harm might be. In recent years, both concepts have been integrated (for risk and medical devices). For instance, the ISO 31000:2018 publication suggests that risk is about 'uncertainty on objectives' [17], whereas the USA Food and Drug Administration (FDA) adopts the principle that a medical device is an instrument intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease (Federal Food, Drug, and Cosmetic Act (FD&C Act) (Link: https://www.fda.gov/regulatory-information/laws-enforced-fda/federal-food-drug-and-cosmetic-act-fdc-act, accessed on 19 June 2023) [16,83]).

4.1. Particularities of IoT Relevant to RA

One key issue in any RA concerns its *quantification*. NIST suggests using qualitative metrics (i.e., low, medium, high) when addressing likelihood and impacts in risk models [40], which risks multiple interpretations and abstractions and a lack of precision as managers might consider different aspects when determining perceived risks associated with threats. Current RA approaches might fail in IoT due to this dynamic nature, as prior assessments could quickly become obsolete when new devices emerge in networks with different requirements, technologies, objectives, and capabilities. As pointed out in a previous study [40], an effective RA requires predicting devices that could ingress into networks before the assessment, which is highly challenging.

A round of discussion with professionals in the industry on the benefits and shortcomings of RA in IoT unveiled interesting points [41], including the following:

- Incorporate security in early designs through effective shift-left approaches within DevOps [94], i.e., addressing security-related concerns since system specification.
- Quantification of risk is not trivial to accomplish, as the industry still favours qualitative measures (e.g., low, medium and high, as suggested by NIST).
- Careful thinking on how to balance dynamism, automation and human aspects when enacting effective RA in complex environments characterised by frequent connection requests and disconnections.
- Addressing new emerging risks in partially unknown systems; this occurs when potentially malicious devices participating in the network demand service or interactions to act as stepping stones to larger cyber-attacks.

The authors mention in their final remarks one critical point that remains neglected in RA frameworks and methodologies: the industry still believes in the *"perceived infeasibility of fully automated risk assessment in the IoT"*, mostly due to the issues raised throughout this paper, namely dynamism and temporality.

IoT is a technological solution to address many problems in communicating information across multiple CPS and IS, with applications ranging from industry, healthcare and smart infrastructure, to mention a few. The dynamics and temporality of connections among devices distinguish IoT from other systems and services [95]. Next, we comment on the challenges in highly interconnected networks in IoT/MIoT, including:

- Quantification of the communication of information to other devices that are aligned with the organisation's risk appetite and its scale when accommodating many interacting devices.
- Clear shortcomings of *periodic* RA that do not account for unknown system boundaries, latest vulnerabilities (as advertised by vendors and security-oriented organisations), and failure to recognise that IoT-based assets are sometimes the initiators or the promoters of larger attacks [41].
- Lack of rigorous *dynamic* risk approaches [40] that are instead substituted by *periodic* assessment approaches.
- Accounting devices with different capabilities and objectives, i.e., sets requiring connections to happen only once or twice, as well as persistent connections and unsigned devices seeking to connect with signed/authorised devices that represent increases in risk and likelihood of attacks.
- Consideration of the heterogeneity of devices interacting in healthcare-related IoT/MIoT ecosystems.

- The need for *automated, continuous and collaborative* RA coupled with supporting tools based on simulation and modelling to enhance the understanding of which new devices might emerge in networks, what they might request or perform, and communication patterns that could be developed through time.

The most commonly desired properties of systems deployed to end-users include robustness, resilience (ability to retain operation even in the presence of catastrophic events), performance, and usability. Regarding MIoT, security officers also consider safety, privacy, seamless system-wide integration, and interoperability with other systems. This is especially relevant when we consider healthcare settings where MIoT designers tailor their systems and interfaces to accommodate vulnerable patients, i.e., elderly, undergoing recovery (post-procedure or after surgery), pregnant women experiencing discomfort or undergoing following up, as well as non-human counterparts, e.g., hospital equipment, beds, and infrastructure to sustain IS and services.

Standard protections include encryption for communication and storage, security systems, such as IDS and firewalls, and raising awareness of cyber security and the most likely threats facing stakeholders. Under a comprehensive and scaled MIoT setting, we focus on sophisticated, hard-to-track or identify cyber-attacks posed by advanced threat actors. The plethora of healthcare devices and their inherent characteristics play an important role in detecting and thwarting cyber-attacks before they propagate over other systems and networks.

Figure 2 depicts a typical MIoT ecosystem illustrating how hospital healthcare management and cyber security systems may be integrated. It shows how a DRA proposition could work and the necessary underpinning features and considerations to be effective. It is worth noting that, throughout any MIoT/IoT life-cycle, there are interactions with third-party devices and a myriad of participants (both 'normal' and malicious users), where the communication patterns could symbolise cyber-attacks, but, in fact, represent incompetent use or accidental actions. It is the job of security officers to differentiate these behaviours and to confirm or refute cyber-attacks on-the-fly to protect end-users and offer valuable user experience whilst using the technologies.

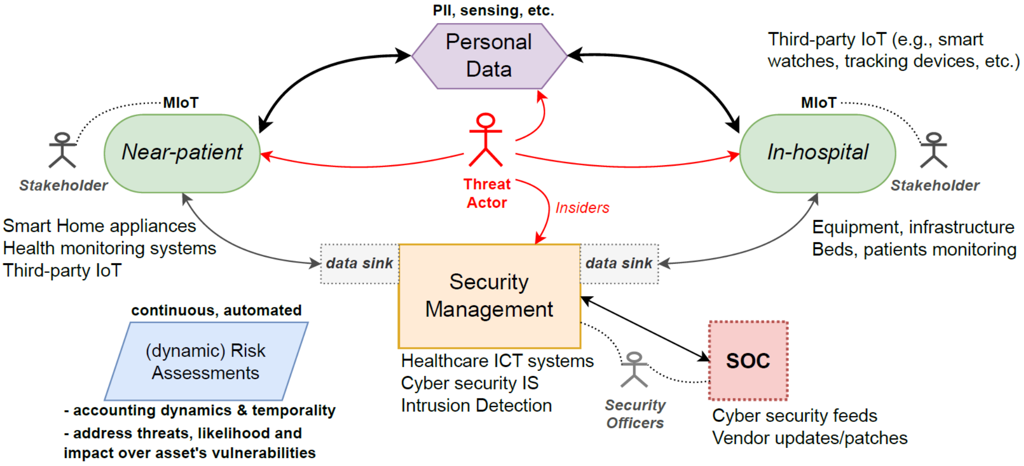

Figure 2. General MIoT ecosystem and the issues surrounding DRA propositions.

The figure also shows that the solution must work with existing cyber security and information and communications technology (ICT) systems in hospitals coupled with existing security operational centres (SOC) and then account for the myriad of potential MIoT that will participate in the network. The *data sinks* involve data gathering and may encompass other systems and technologies so that they can function seamlessly and securely, relaying data across public and private networks. SOC has access to all ICT-related systems that utilise dashboards extensively to observe the entire attack surface and continuously monitor the network's health to direct responses (mitigations in the case of attacks) and to perform remote management of distributed assets. Within this framework, sophisticated threat actors continuously inspect networks for vulnerabilities on any level, i.e., near-patient and in-hospital.

4.2. Similar RA Approaches Specific to IoT

Sicari et al. (2018) [96] proposed a risk analysis methodology tailored to end-to-end systems considering the whole data life-cycle of IoT. It accounts for both static and dynamic features of IoT-based systems to tackle risks throughout layers of data flow. The authors suggest five steps to follow: (i) Identify and model a threat as an attack tree, listing the possible attack vectors towards the threat realisation and identifying the principal vulnerabilities (as leaves); (ii) Map to each vulnerability a qualitative exploitability level translated to a quantitative numerical value within (0:10); (iii) Generate a graph highlighting all dependencies among the identified vulnerabilities; (iv) Compute an exploitability value for all the edges of the graph; (v) Account for dependencies by updating the model following iterative formulas. When considering a dynamic risk approach, however, the methodology lacks a support tool to devise the attack trees and graphs and all the required updates. The mechanism provided is interesting in mapping potential vulnerabilities over IoT assets and converting qualitative scales to quantitative values.

Abie and Balasingham (2012) [97] considered autonomous IoT that requires a risk-based adaptive assessment framework for risk analysis that can sustain predictions for impending issues regarding assets, impact prediction, implementing planned actions for mitigation and reducing risk exposure [41]. They proposed the adaptation of two models for predicting uncertainty, namely, Cyber Value at Risk (CVR) [98] and MicroMort [99], and a mechanism to compute the economic impact of IoT risks. The authors proposed quantifying uncertainties in IoT domains, identifying the most likely attack vectors and combining risk approaches. The manual alternative does not account for any dynamics and changes in attack surface as multiple IoT participate in networks.

Matheu-García et al. (2019) [100] suggest using a certification methodology that combines security risk assessment with security testing to certify devices across application contexts. The proposed approach is derived from ETSI (based on ISO 31000 and ISO 29119) and extended to include labelling activities to address certification and tackle security risks related to IoT domains. The work calculates base scores for each identified vulnerability employing a common vulnerability scoring system (CVSS) formula. It proposes an approach to quantifying risks in IoT environments by integrating different standards with known scoring systems; however, it does not address any system dynamics or changes in the attack surface over time, which represent fundamental characteristics of these systems.

Formal approaches for modelling and assessing IoT security have been proposed, for instance, by Ge et al. (2017) [101], who combined a hierarchical attack representation model (HARM) to evaluate it using the known symbolic hierarchical automated reliability and performance evaluator (SHARPE). In contrast, Mohsin et al. (2017) [85] devised IoTRiskAnalyzer to analyse risks using a quantitative probabilistic model-checking approach. These techniques, unfortunately, fall short of the required abstractions to represent complex MIoT, as they must analyse a massive state space when modelling. These shortcomings are alleviated by probabilistic model checking that sustains partial state space analysis; however, these problems will still be present in over-scaled MIoT/IoT networks.

Finally, we mention the work of Duan et al. (2021) [102] who implemented an end-to-end assessment framework for IoT, consisting of a vulnerability assessment model equipped with visualisation using AI/ML to process vulnerability descriptions and predict severity scores. The proposed framework has four phases: (i) generation of a system model comprising specifications of smart devices and connectivity information; (ii) data processing using AI/ML integrated with known vulnerability catalogues, namely, the National Vulnerability Database (NVD) maintained by NIST; (iii) adoption of a graphical security model based on a two-layer HARM methodology; and (iv) a visualisation interface to present the assessment results. A drawback is that the approach is static and requires frequent changes given the inherent dynamics of IoT networks.

4.3. Discussion

A substantial amount of research has addressed the difficulties posed by *quantifying risk*, a common theme with regard to risk in general. There are also attempts to integrate risk frameworks with cyber security catalogues, usually maintained by the community, that update discovered vulnerabilities, so that managers can take preventive actions to tackle cyber-attacks. We have summarised vital factors when tackling dynamic RA in MIoT ecosystems, as follows:

- Improvement in the identification of the potential attack surface posed by dynamic IoT-based assets in complex networks [35].
- Tackling the dynamics and temporality of transient and intermittent behaviours characteristic of MIoT environments. Account for the inherent complexities of performing these tasks in (near) real-time settings.
- Adherence to MIoT/IoT-specific guidance and regulations, aligning them to hospital technologies, equipment and communication protocols.
- Effective and seamless TM in early designs when considering MIoT as a technological solution to encompass other IS/ICT in place and aligned with SOC objectives.
    - One interesting approach supported by OWASP is to employ a tool called `pytm` (OWASP pytm, a Pythonic framework for TM: https://owasp.org/www-project-pytm/, accessed on 19 June 2023). It helps stakeholders to build a textual representation of a business setting or environment and to generate a DFD or a sequence diagram to highlight the most likely threats within the system.
- Account and adapt to dynamic attack surface and third-party equipment that is in contact with MIoT over its life-cycle.
- Employ and incorporate known and community-driven vulnerability catalogues and cyber intelligence feeds.
- Enhance cyber security awareness and personnel training with regards to the latest cyber-attacks and threats to improve preparedness, tackle mitigations and pro-actively protect MIoT/IoT-based services and systems.
- Better visualise attacks [101,103] to understand threat actor's progression over IoT-based assets.

Security is an all-encompassing problem faced by all organisations. With regard to managerial implications for the healthcare domain, we highlight the need for asset visibility, where SOC operators understand cyber-attack repercussions as they progress in the networks [90,104,105]. Zhang and Navimipour (2022) [106] discuss IoT-based medical management systems and inherent open issues. Modern SOC should take multiple data feeds to provide context and to undermine cyber-attacks as they happen. Standard services implemented by SOC include event and incident management and response, dispatching teams to solve issues, user behaviour analytics, cyber threat intelligence, vulnerability management, and risk assessment. Nowadays, the trend is towards automating the processes of triaging multiple data for effective and timely analysis, tool integration, and adherence to regulation and guidance by established cyber security institutions (e.g., the US' NIST, the EU's ENISA, or the UK's NCSC). Security officers must orchestrate these systems to work together by performing relevant and timely risk assessments.

There has been substantial research relating to DRA in isolation without considering its applicability to IoT.

For instance, Riesco and Villagrá (2019) [107] employed cyber threat intelligence (CTI) combined with DRA using so-called *semantic reasoners* to enact realistic RA and to support decision-making. The approach used standardised intelligence specifications so that a broader community could participate in the security effort. Another example is provided by Antonello et al. (2022) [108]. They suggested performing DRA using modelling and simulation combined with systems theory, providing a systematic analysis approach for studying dynamic scenarios.

An interesting study by Kavallieratos et al. (2019) [26] focused on TM applied to smart home ecosystems. The authors identified information (user credentials, data collection, status information, logs, media, location, and PII) and physical assets (IoT devices, hubs, gateways, sensors/actuators, cloud servers). Then they developed DFD models to represent interactions and analysed the system using STRIDE. The consideration of dynamic approaches is a multi-factor problem that involves multiple research areas. In order to work towards better usability and user experience for risk analysis, Collen et al. (2022) [109] employed a user-friendly interface to guide DRA, appending iterative feedback directed at non-technical users. The authors suggested ways to create decision-making trees to add transparency to decisions focusing on the smart home.

Figure 3 shows a comparative analysis between traditional RA and DRA. It showcases the main RA objectives in contrast with DRA, aiming to derive automated, continuous, and collaborative tasks throughout the IoT/MIoT ecosystem. For each aspect, it lists frameworks and cyber security concepts to factor in when incorporating DRA in solutions. Specifically, with respect to MIoT, DRA must seamlessly track activities and process data to determine 'under attack' situations or events that pose a substantial risk to patients. One significant idea is to not only deduplicate entries across multiple datasets, but to triage them in a way that helps the decision-making process enact timely protective measures for end-users by denying access momentarily or blocking devices until further notice.

As mentioned earlier, there are non-trivial challenges to address in such complex environments posed by the sheer scale of MIoT networks. Organisations need to acknowledge that current RA methodologies are often reviewed only periodically and at an undesirable pace. We envision opportunities in risk analysis to address these considerations and adapt current frameworks to withstand stricter security requirements as demanded by MIoT technologies. Researchers working with IoT/MIoT could seek to understand the techniques and methodologies employed by researchers working with DRA in other contexts and then adapt them to work with the observed healthcare requirements.

Finally, we highlight the use of *automation* to address cyber security tasks in the massive and dynamic settings presented by IoT/MIoT networks with multiple owners, vendors, and stakeholders. Given the massive amount of data that can potentially be produced hourly from sensors, IS, monitoring applications and tracking devices, compounded by the fact that sophisticated algorithms require quality data to make timely predictions and decisions, the level of automation for IoT-based solutions will dictate its effectiveness in combatting cybercrime-related risks to the infrastructure. Admittedly, automation comes with trade-offs and, if poorly executed, can pose negative impacts to organisations. For instance, automated systems may produce more data than they can handle (i.e., data deluge), or triage and remove more entries than required (e.g., whilst handling outliers), or sophisticated threat actors may influence the algorithms using advanced data poisoning techniques.

Figure 4 illustrates the risks and exposures that are potentially created for end-users or patients in IoT/MIoT settings. The figure indicates the usual attack vectors present in this kind of infrastructure and also highlights how dynamic behaviours triggered by sophisticated threat actors may impact the end-user of the technology and undermine trust in systems and services. It is worth mentioning that, as discussed throughout this work, other risks are not mapped due to lack of knowledge and uncertainty as to novel attack venues that can be employed by cyber-attackers. End-users and patients want to use MIoT devices due to the high service-level aggregated value that they offer; however, they also want to be safeguarded from unwanted intrusions and cyber-attacks directed at the equipment.

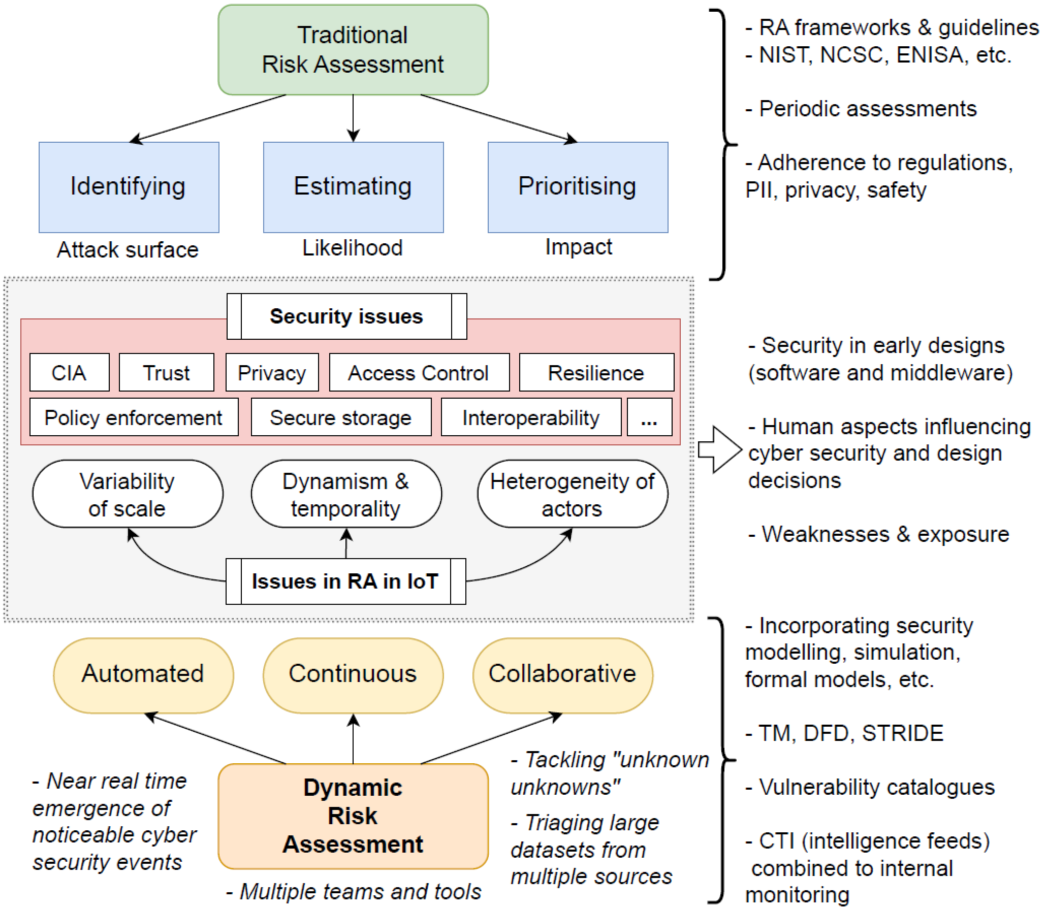
Traditional Risk Assessment
Identifying
Estimating
Prioritising
Attack surface
Likelihood
Impact
- RA frameworks & guidelines
- NIST, NCSC, ENISA, etc.
- Periodic assessments
- Adherence to regulations, PII, privacy, safety
Security issues
CIA
Trust
Privacy
Access Control
Resilience
Policy enforcement
Secure storage
Interoperability
...
Variability of scale
Dynamism & temporality
Heterogeneity of actors
Issues in RA in IoT
- Security in early designs (software and middleware)
- Human aspects influencing cyber security and design decisions
- Weaknesses & exposure
Automated
Continuous
Collaborative
Dynamic Risk Assessment
- Near real time emergence of noticeable cyber security events
- Multiple teams and tools
- Tackling "unknown unknowns"
- Triaging large datasets from multiple sources
- Incorporating security modelling, simulation, formal models, etc.
- TM, DFD, STRIDE
- Vulnerability catalogues
- CTI (intelligence feeds) combined to internal monitoring

Figure 3. Comparative analysis contrasting traditional RA with DRA propositions.

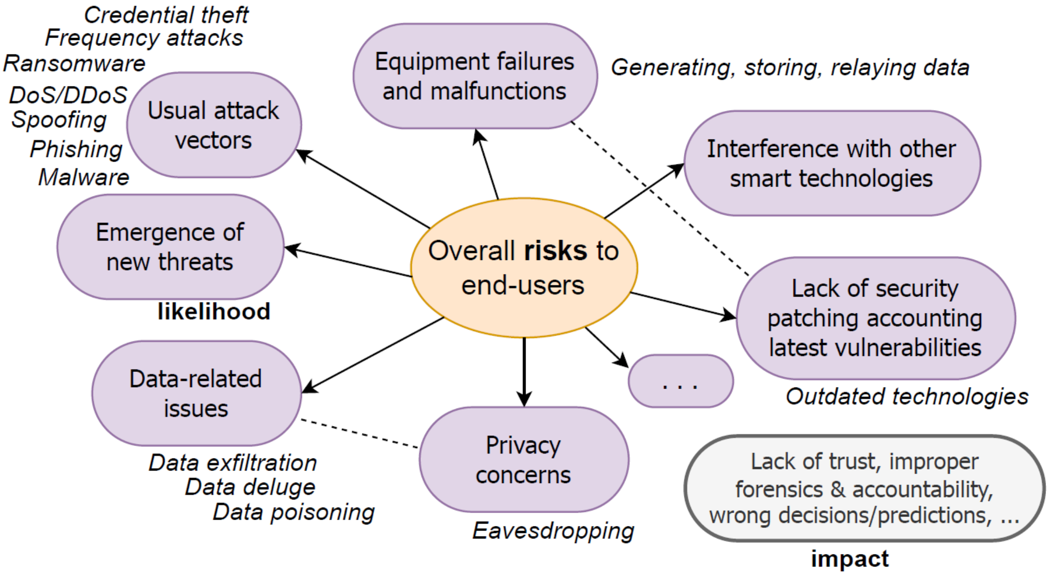
Credential theft
Frequency attacks
Ransomware
DoS/DDoS
Spoofing
Phishing
Malware
Usual attack vectors
Equipment failures and malfunctions
Generating, storing, relaying data
Interference with other smart technologies
Emergence of new threats
likelihood
Overall risks to end-users
Lack of security patching accounting latest vulnerabilities
. . .
Outdated technologies
Data-related issues
Data exfiltration
Data deluge
Data poisoning
Privacy concerns
Eavesdropping
Lack of trust, improper forensics & accountability, wrong decisions/predictions, ...
impact

Figure 4. Overall risks to end-users posed by IoT/MIoT settings.

5. Conclusions

Our objective was to consider the foremost challenges with respect to DRA in MIoT and how managers and developers across the ecosystem can deal with emergent patient risks when employing wearable computing in healthcare settings. The contributions of the paper included presentation of an SLR outlining current trends and existing approaches, and provision of recommendations on how to address the impact of intrusions and mitigations to protect end-users. The work discussed risks associated with using MIoT and enumerated approaches to protection when working with these technologies. In the meta-analysis associated with the SLR, we sought to broaden understanding of how healthcare settings can tackle risks using MIoT/IoT. We were interested in detailing how these organisations have applied RA effectively and the operational issues associated with addressing emergent risks for improving patient care.

It is undoubtedly true that cyber security offers end-users a protective layer with controls that can prevent data leakage, protect PII, and ensure smooth use and data storage of confidential information. It may also efficiently thwart, prevent, or respond to cyber-attacks or malicious circumstances arising in MIoT networks, tackling threats and preventing them from cascading to other systems. The problem we have identified when employing MIoT devices to track patients' healthcare is how to differentiate local measurement deviations and anomalies from actual cyber-attacks. The healthcare architecture needs to be improved by developing a framework on top of the basic functionalities that prevent unwarranted cyber-attacks. The idea is to improve architecture resilience properties so that the limited hardware of a device can generate valuable data even under duress and with the overhead needed to support these capabilities.

Future Work and Research Directions

In this research area there are numerous opportunities for improvements with respect to privacy, safety, and cyber security. For instance, we envision the incorporation of CTI into the dynamic and automated RA effort in IoT, as discussed in previous work on applications in Industry 4.0 [110], and, more generically, to smart devices [111]. Moreover, we cannot dismiss the benefits and strengths of AI/ML (and related approaches, e.g., deep learning [112], and so on) in cyber security applied to RA in MIoT/IoT [113–116]. The combination of these approaches with security analysis allows risk analysts to enhance decision making and predictive capabilities, enabling them to anticipate and withstand cyber-attacks before they develop in systems and networks. These approaches, however, require further investigation to determine their usefulness in real-world settings and to understand the complex infrastructure, behaviours, and interactions.

As Nurse et al. (2017) [40] have outlined, future RA approaches must be coupled with simulation and modelling to enhance the predictive nature of massive IoT/MIoT dynamics (arrival/departure) and temporality. In this sense, a digital twins approach, where virtual and physical counterparts devise a model for thorough analysis, is one way to improve prediction. Our investigation has also identified how the use of modern approaches, such as cloud and fog computing [117–119], in healthcare can help patients receive better care whilst seamlessly protecting their data and equipment. We have argued that these approaches need more timely analysis features, as the abstraction demanded to compute numerical indices sometimes hinders decision-making capabilities due to the sheer complexity of the potential state space posed by MIoT/IoT. Despite these shortcomings, we believe that advancements in digital twins applied to healthcare [120,121], where physical and virtual counterparts interact, offers realistic opportunities to enhance the analysis and understanding of attack progression. These provisions, coupled with standards recognised by the industry [122], can help healthcare stakeholders offer better service levels to patients. The ability to integrate virtual and physical elements has huge potential for answering complex *'what if?'* questions in massive attack surfaces, such as those posed by MIoT/IoT.

Author Contributions: Conceptualisation, R.M.C., P.G., C.M., F.H. and S.C.C.; methodology, R.M.C., P.G., C.M., F.H. and S.C.C.; validation, R.M.C., P.G., C.M., F.H. and S.C.C.; formal analysis, R.M.C., P.G., C.M., F.H. and S.C.C.; investigation, R.M.C., P.G., C.M., F.H. and S.C.C.; resources, R.M.C., P.G., C.M., F.H. and S.C.C.; data curation, R.M.C., P.G., C.M., F.H. and S.C.C.; writing—original draft preparation, R.M.C.; writing—review and editing, R.M.C., P.G., C.M., F.H. and S.C.C.; visualisation, R.M.C., P.G., C.M., F.H. and S.C.C.; supervision, R.M.C., P.G., C.M., F.H. and S.C.C.; project administration, R.M.C., P.G., C.M., F.H. and S.C.C.; funding acquisition, R.M.C., P.G., C.M. and F.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by FAPERGS/RS/Brazil under call CONFAP—UK ACADEMIES, grant reference: 22/2551-0001368-6.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: SLR analysis data: https://github.com/czekster/SLR-miot, accessed on 19 June 2023.

Acknowledgments: We thank our respective academic institutions for supporting this research.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

AAL	Ambient Assisted Living
AI/ML	Artificial Intelligence and Machine Learning
BAG	Bayesian Attack Graphs
CCTA	Central Communication and Telecommunication Agency
CIA	Confidentiality, Integrity, Availability
CKC	Cyber Kill Chain
CMMI	Capability Maturity Model Integration
CPS	Cyber-Physical System
CRAMM	CCTA Risk Analysis and Management Method
CTI	Cyber Threat Intelligence
CVR	Cyber Value at Risk
CVSS	Common Vulnerability Scoring System
DFD	Data Flow Diagram
DLT	Distributed Ledger Technologies
DNS	Domain Name System
DNSSEC	DNS SECurity extensions
DDoS/DoS	Distributed Denial-of-Service
DRA	Dynamic Risk Assessment
DREAD	Damage, Reproducibility, Exploitability, Affected Users, Discoverability
DSE	Design Space Exploration
EBIOS	*Expression des Besoins et Identification des Objectifs de Sécurité* (FR)
EHR	Electronic Health Records
EMR	Electronic Medical Recording
ENISA	European Union Agency for Cybersecurity (EU)
ETSI	European Telecommunications Standards Institute
EU	European Union
FDA	Food and Drug Administration (US)
GDPR	General Data Protection Regulation
HARM	Hierarchical Attack Representation Model
HIoT	Health Internet of Things
HIPAA	Health Insurance Portability and Accountability Act
HPA	Health Prescription Assistant
ICT	Information and Communications Technology
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IIoT	Industrial IoT
IoHT	Internet of Health Things
IoMT	Internet of Medical Things
IoT	Internet-of-Things
IOTA	IoT Application
IS	Information Systems
ISO	International Organization for Standardization
MIoT	Medical Internet-of-Things
MVL	Multiple-Valued Logic
NCSC	National Cyber Security Centre (UK)

NHS	National Health Service
NIST	National Institute of Standards and Technology (US)
NVD	National Vulnerability Database (NIST/US)
OCS	Order Communication Systems
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OWASP	Open Worldwide Application Security Project
PACS	Picture Archiving and Communication Systems
PASTA	Process for Attack Simulation and Threat Analysis
PET	Privacy Enhancing Technologies
PHI	Patient Health Information
PII	Personally and Identifiable Information
PIR	Private Information Retrieval
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RA	Risk Assessment
RAP	Risk Assessment Process
RTL	Real-time Location Services
SHARPE	Symbolic Hierarchical Automated Reliability and Performance Evaluator
SIEM	Security Information and Event Management
SLR	Systematic Literature Review
SOC	Security Operational Centre
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, DoS, Elevation of Privilege
TARA	Threat Assessment and Remediation Analysis
TLS	Transport Layer Security
TM	Threat Modelling
VPN	Virtual Private Networks
WBAN	Wireless Body Area Networks

Appendix A. Definitions

Appendix A.1. Risk

According to ISO 31000:2018 [17], risk is “uncertainty on objectives”. NIST’s glossary (NIST Computer Security Research Center Glossary (CSRC): https://csrc.nist.gov/glossary, accessed on 19 June 2023) and publication NIST SP 800-30 Rev-1 [18] states that *“Risk arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts on organizational operations and assets, individuals, other organizations, and the Nation”.*

Appendix A.2. Medical Device

ANSI/AAMI/ISO 14971:2007 standard [93] states that a medical device is *“any instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material, or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific purpose(s) of (i) diagnosis, prevention, monitoring, treatment or alleviation of disease, (ii) diagnosis, monitoring, treatment, alleviation of or compensation for an injury, (iii) investigation, replacement, modification, or support of the anatomy or of a physiological process, (iv) supporting or sustaining life, (v) control of conception, (vi) disinfection of medical devices, (vii) providing information for medical purposes by means of in vitro examination of specimens derived from the human body, and which does not achieve its primary intended action in or on the human body by pharmacological, immunological, or metabolic means, but which may be assisted in its function by such means”.*

Appendix A.3. Standards and guidance

These are relevant standards and guidance related to risk, medical devices and health software.

- **ISO/IEC 27000:2018**: Information technology—Security techniques—Information security management systems—Overview and vocabulary (https://www.iso.org/standard/73906.html, accessed on 19 June 2023)

- **IEC 62304:2006**: Medical device software—Software life cycle processes (https://www.iso.org/standard/38421.html, accessed on 19 June 2023)
- **ISO/IEC 27032:2012**: Information technology—Security techniques—Guidelines for cybersecurity (https://www.iso.org/standard/44375.html, accessed on 19 June 2023)
- **IEC 82304-1:2016**: Health software—Part 1: General requirements for product safety (https://www.iso.org/standard/59543.html, accessed on 19 June 2023)
- **IEC 80001-1:2021**: Application of risk management for IT-networks incorporating medical devices—Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software (https://www.iso.org/standard/72026.html, accessed on 19 June 2023)
- **IEC/TR 80001-2-2:2012**: Application of risk management for IT-networks incorporating medical devices—Part 2-2: Guidance for the communication of medical device security needs, risks and controls (https://www.iso.org/standard/57939.html, accessed on 19 June 2023)
- **IEC/TR 80002-1:2009**: Medical device software—Part 1: Guidance on the application of ISO 14971 to medical device software (https://www.iso.org/standard/54146.html, accessed on 19 June 2023)
- **ISO/TR 80002-2:2017**: Medical device software—Part 2: Validation of software for medical device quality systems (https://www.iso.org/standard/60044.html, accessed on 19 June 2023)
- **IEC/TR 80002-3:2014**: Medical device software—Part 3: Process reference model of medical device software life cycle processes (IEC 62304) (https://www.iso.org/standard/65624.html, accessed on 19 June 2023)
- **ISO/IEC 30141:2018**: Internet of Things (IoT)—Reference Architecture (https://www.iso.org/standard/65695.html, accessed on 19 June 2023)
- **ETSI TS 103 645 V2.1.2 (2020-06)**: CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements (https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf, accessed on 19 June 2023)
- **NIST SP 1800-36**: Trusted IoT Device Network-Layer Onboarding and Lifecycle Management (https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management, accessed on 19 June 2023)

References

1. Dimitrov, D.V. Medical internet of things and big data in healthcare. *Healthc. Inform. Res.* **2016**, *22*, 156–163. [CrossRef] [PubMed]
2. Haghi, M.; Thurow, K.; Stoll, R. Wearable devices in medical internet of things: Scientific research and commercially available devices. *Healthc. Inform. Res.* **2017**, *23*, 4–15. [CrossRef] [PubMed]
3. Meneghello, F.; Calore, M.; Zucchetto, D.; Polese, M.; Zanella, A. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet Things J.* **2019**, *6*, 8182–8201. [CrossRef]
4. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-physical systems security—A survey. *IEEE Internet Things J.* **2017**, *4*, 1802–1831. [CrossRef]
5. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the IEEE 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 4–16 December 2015; pp. 336–341.
6. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
7. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and privacy in the medical internet of things: A review. *Secur. Commun. Netw.* **2018**, *2018*, 1–9. [CrossRef]
8. Noor, M.b.M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]
9. Pradhan, B.; Bhattacharyya, S.; Pal, K. IoT-based applications in healthcare devices. *J. Healthc. Eng.* **2021**, *2021*, 1–18. [CrossRef]
10. Javaid, M.; Khan, I.H. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *J. Oral Biol. Craniofac. Res.* **2021**, *11*, 209–214. [CrossRef]
11. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
12. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258. [CrossRef]

13. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* **2018**, *38*, 8–27. [CrossRef]
14. Schwartz, P.M.; Solove, D.J. The PII problem: Privacy and a new concept of personally identifiable information. *NYUL Rev.* **2011**, *86*, 1814.
15. Alsubaei, F.; Abuhussein, A.; Shiva, S. Security and privacy in the internet of medical things: Taxonomy and risk assessment. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9 October 2017; pp. 112–120.
16. Malamas, V.; Chantzis, F.; Dasaklis, T.K.; Stergiopoulos, G.; Kotzanikolaou, P.; Douligeris, C. Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal. *IEEE Access* **2021**, *9*, 40049–40075. [CrossRef]
17. *ISO 31000:2018*; Risk Management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/65694.html (accessed on 19 June 2023).
18. *800-30 REV. 1*; Guide for Conducting Risk Assessments. NIST Joint Task Force Transformation Initiative: Washington, DC, USA, 2012. Available online: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (accessed on 19 June 2023).
19. Caralli, R.A.; Stevens, J.F.; Young, L.R.; Wilson, W.R. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*; Technical Report; Software Engineering Institute—Carnegie Mellon University: Pittsburgh, PA, USA, 2007.
20. Gritzalis, D.; Iseppi, G.; Mylonas, A.; Stavrou, V. Exiting the risk assessment maze: A meta-survey. *ACM Comput. Surv. CSUR* **2018**, *51*, 1–30. [CrossRef]
21. Zio, E. The future of risk assessment. *Reliab. Eng. Syst. Saf.* **2018**, *177*, 176–190. [CrossRef]
22. Collen, A.; Nijdam, N.A. Can I Sleep Safely in My Smarthome? A Novel Framework on Automating Dynamic Risk Assessment in IoT Environments. *Electronics* **2022**, *11*, 1123. [CrossRef]
23. Datta, S.K. DRAFT-A Cybersecurity Framework for IoT Platforms. In Proceedings of the IEEE 2020 Zooming Innovation in Consumer Technologies Conference (ZINC), Novi Sad, Serbia, 26–27 May 2020; pp. 77–81.
24. Nurse, J.R.; Atamli, A.; Martin, A. Towards a usable framework for modelling security and privacy risks in the smart home. In *Human Aspects of Information Security, Privacy, and Trust: 4th International Conference, HAS 2016, Held as Part of HCI International 2016, Toronto, ON, Canada, 17–22 July 2016*; Springer: Cham, Switzerland, 2016; pp. 255–267.
25. Pandey, P.; Collen, A.; Nijdam, N.; Anagnostopoulos, M.; Katsikas, S.; Konstantas, D. Towards automated threat-based risk assessment for cyber security in smarthomes. In Proceedings of the 18th European Conference on Cyber Warfare and Security (ECCWS 2019), Coimbra, Portugal, 4–5 July 2019; pp. 4–5.
26. Kavallieratos, G.; Gkioulos, V.; Katsikas, S.K. Threat analysis in dynamic environments: The case of the smart home. In Proceedings of the IEEE 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019; pp. 234–240.
27. HaddadPajouh, H.; Dehghantanha, A.; Parizi, R.M.; Aledhari, M.; Karimipour, H. A survey on internet of things security: Requirements, challenges, and solutions. *Internet Things J.* **2021**, *14*, 100129. [CrossRef]
28. Sridharan, C. *Distributed Systems Observability: A Guide to Building Robust Systems*; O'Reilly Media: Sebastopol, CA, USA, 2018.
29. Möller, D.P. Threats and Threat Intelligence. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices*; Springer: Cham, Switzerland, 2023; pp. 71–129.
30. Susskind, N.G. Cybersecurity compliance and risk management strategies: What directors, officers, and managers need to know. *N. Y. Univ. J. Law Bus.* **2014**, *11*, 573.
31. Bhuiyan, M.N.; Rahman, M.M.; Billah, M.M.; Saha, D. Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet Things J.* **2021**, *8*, 10474–10498. [CrossRef]
32. Arasteh, H.; Hosseinnezhad, V.; Loia, V.; Tommasetti, A.; Troisi, O.; Shafie-khah, M.; Siano, P. Iot-based smart cities: A survey. In Proceedings of the 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), Florence, Italy, 7–10 June 2016; pp. 1–6.
33. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
34. Islam, S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The internet of things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]
35. Rizvi, S.; Orr, R.; Cox, A.; Ashokkumar, P.; Rizvi, M.R. Identifying the attack surface for IoT network. *Internet Things J.* **2020**, *9*, 100162. [CrossRef]
36. UcedaVelez, T.; Morana, M.M. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*; John Wiley & Sons: Hoboken, NJ, USA, 2015.
37. Wolf, A.; Simopoulos, D.; D'Avino, L.; Schwaiger, P. The PASTA threat model implementation in the IoT development life cycle. *Informatik* **2021**, *2020* .
38. Kalinin, M.; Krundyshev, V.; Zegzhda, P. Cybersecurity risk assessment in smart city infrastructures. *Machines* **2021**, *9*, 78. [CrossRef]
39. Malik, A.A.; Tosh, D.K. Dynamic Risk Assessment and Analysis Framework for Large-Scale Cyber-Physical Systems. *EAI Endorsed Trans. Secur. Saf.* **2022**, *8*, 1. [CrossRef]
40. Nurse, J.R.; Creese, S.; De Roure, D. Security risk assessment in Internet of Things systems. *IT Prof.* **2017**, *19*, 20–26. [CrossRef]

41. Nurse, J.R.; Radanliev, P.; Creese, S.; De Roure, D. If you can't understand it, you can't properly assess it! The reality of assessing security risks in Internet of Things systems. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT, London, UK, 28–29 March 2018.
42. Tarandach, I.; Coles, M.J. *Threat Modeling: A Practical Guide for Development Teams*, 1st ed.; O'Reilly Media: Sebastopol, CA, USA, 2020; ISBN-13: 978-1492056553.
43. Shevchenko, N.; Chick, T.A.; O'Riordan, P.; Scanlon, T.P.; Woody, C. *Threat Modeling: A Summary of Available Methods*; Technical Report; Software Engineering Institute—Carnegie Mellon University: Pittsburgh, PA, USA, 2018.
44. Yskout, K.; Heyman, T.; Van Landuyt, D.; Sion, L.; Wuyts, K.; Joosen, W. Threat modeling: From infancy to maturity. In Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering: New Ideas and Emerging Results, Seoul, Republic of Korea, 27 June–19 July 2020; pp. 9–12.
45. Omotosho, A.; Ayemlo Haruna, B.; Mikail Olaniyi, O. Threat modeling of internet of things health devices. *J. Appl. Secur. Res.* **2019**, *14*, 106–121. [CrossRef]
46. Abbas, S.G.; Vaccari, I.; Hussain, F.; Zahid, S.; Fayyaz, U.U.; Shah, G.A.; Bakhshi, T.; Cambiaso, E. Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach. *Sensors* **2021**, *21*, 4816. [CrossRef]
47. Faily, S.; Scandariato, R.; Shostack, A.; Sion, L.; Ki-Aries, D. Contextualisation of data flow diagrams for security analysis. In *Graphical Models for Security: 7th International Workshop, GraMSec 2020, Boston, MA, USA, 22 June 2020*; Springer: Cham, Switzerland, 2020; pp. 186–197.
48. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of medical things security assessment framework. *Internet Things J.* **2019**, *8*, 100123. [CrossRef]
49. Alamri, B.; Crowley, K.; Richardson, I. Cybersecurity Risk Management Framework for Blockchain Identity Management Systems in Health IoT. *Sensors* **2022**, *23*, 218. [CrossRef] [PubMed]
50. Rodrigues, J.J.; Segundo, D.B.D.R.; Junqueira, H.A.; Sabino, M.H.; Prince, R.M.; Al-Muhtadi, J.; De Albuquerque, V.H.C. Enabling technologies for the internet of health things. *IEEE Access* **2018**, *6*, 13129–13141. [CrossRef]
51. Da Costa, C.A.; Pasluosta, C.F.; Eskofier, B.; Da Silva, D.B.; da Rosa Righi, R. Internet of health things: Toward intelligent vital signs monitoring in hospital wards. *Artif. Intell. Med.* **2018**, *89*, 61–69. [CrossRef] [PubMed]
52. Jaigirdar, F.T.; Rudolph, C.; Bain, C. Can I trust the data I see? A Physician's concern on medical data in IoT health architectures. In Proceedings of the Australasian Computer Science Week Multiconference, Sydney, Australia, 29–31 January 2019; pp. 1–10.
53. Vishnu, S.; Ramson, S.J.; Jegan, R. Internet of medical things (IoMT)-An overview. In Proceedings of the IEEE 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 5-6 March 2020; pp. 101–104.
54. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet Things J.* **2020**, *8*, 8707–8718. [CrossRef]
55. Joyia, G.J.; Liaqat, R.M.; Farooq, A.; Rehman, S. Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. *J. Commun.* **2017**, *12*, 240–247. [CrossRef]
56. Gaurav, A.; Psannis, K.; Peraković, D. Security of cloud-based medical internet of things (miots): A survey. *Int. J. Softw. Sci. Comput. Intell.* **2022**, *14*, 1–16. [CrossRef]
57. Elhoseny, M.; Thilakarathne, N.N.; Alghamdi, M.I.; Mahendran, R.K.; Gardezi, A.A.; Weerasinghe, H.; Welhenge, A. Security and privacy issues in medical internet of things: Overview, countermeasures, challenges and future directions. *Sustainability* **2021**, *13*, 11645. [CrossRef]
58. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet* **2020**, *12*, 157. [CrossRef]
59. Rajawat, A.S.; Goyal, S.; Bedi, P.; Shrivastava, A.; Constantin, N.B.; Raboaca, M.S.; Verma, C. Security Analysis for Threats to Patient Data in the Medical Internet of Things. In Proceedings of the IEEE 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 16–17 December 2022; pp. 248–253.
60. Nagajayanthi, B. Decades of Internet of Things towards twenty-first century: A research-based introspective. *Wirel. Pers. Commun.* **2022**, *123*, 3661–3697. [CrossRef]
61. Touqeer, H.; Zaman, S.; Amin, R.; Hussain, M.; Al-Turjman, F.; Bilal, M. Smart home security: Challenges, issues and solutions at different IoT layers. *J. Supercomput.* **2021**, *77*, 14053–14089. [CrossRef]
62. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the IEEE 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Tamil Nadu, India, 10–11 February 2017; pp. 32–37.
63. Farahani, B.; Firouzi, F.; Chang, V.; Badaroglu, M.; Constant, N.; Mankodiya, K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Gener. Comput. Syst.* **2018**, *78*, 659–676. [CrossRef]
64. Fagan, M.; Marron, J.; Watrobski, P.; Souppaya, M.; Mulugeta, B.; Symington, S.; Harkins, D.; Barker, W.; Richardson, M. *Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management: Enhancing Internet Protocol-Based IoT Device and Network Security (Preliminary Draft)*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022.
65. Farahani, B.; Firouzi, F.; Luecking, M. The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *J. Netw. Comput. Appl.* **2021**, *177*, 102936. [CrossRef]
66. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and iot integration: A systematic survey. *Sensors* **2018**, *18*, 2575. [CrossRef]

67. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [CrossRef]
68. Novo, O. Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [CrossRef]
69. Yadav, L.; Mitra, M.; Kumar, A.; Bhushan, B.; Al-Asadi, M.A. Nullifying the Prevalent Threats in IoT Based Applications and Smart Cities Using Blockchain Technology. In *Low Power Architectures for IoT Applications*; Springer: Singapore, 2023; pp. 241–261.
70. Popov, S.; Lu, Q. IOTA: Feeless and free. In *IEEE Blockchain Technical Briefs*; Institute of Electrical and Electronics Engineers: Piscataway, NJ, USA, 2019.
71. Alshaikhli, M.; Elfouly, T.; Elharrouss, O.; Mohamed, A.; Ottakath, N. Evolution of Internet of Things from blockchain to IOTA: A survey. *IEEE Access* **2021**, *10*, 844–866. [CrossRef]
72. Conti, M.; Kumar, G.; Nerurkar, P.; Saha, R.; Vigneri, L. A survey on security challenges and solutions in the IOTA. *J. Netw. Comput. Appl.* **2022**, *203*, 103383. [CrossRef]
73. Ullah, I.; De Roode, G.; Meratnia, N.; Havinga, P. Threat modeling—How to visualize attacks on IoTA? *Sensors* **2021**, *21*, 1834. [CrossRef] [PubMed]
74. Argaw, S.T.; Troncoso-Pastoriza, J.R.; Lacey, D.; Florin, M.V.; Calcavecchia, F.; Anderson, D.; Burleson, W.; Vogel, J.M.; O'Leary, C.; Eshaya-Chauvin, B.; et al. Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 146. [CrossRef] [PubMed]
75. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [CrossRef]
76. Ghafur, S.; Kristensen, S.; Honeyford, K.; Martin, G.; Darzi, A.; Aylin, P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. *npj Digit. Med.* **2019**, *2*, 98. [CrossRef] [PubMed]
77. Ghafur, S.; Grass, E.; Jennings, N.R.; Darzi, A. The challenges of cybersecurity in health care: The UK National Health Service as a case study. *Lancet Digit. Health* **2019**, *1*, e10–e12. [CrossRef] [PubMed]
78. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Int. J. Surg.* **2021**, *88*, 105906. [CrossRef] [PubMed]
79. Le, A.; Maple, C.; Watson, T. A Profile-Driven Dynamic Risk Assessment Framework for Connected and Autonomous Vehicles. 2018. Available online: https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0020 (accessed on 19 June 2023)
80. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. Inf. Secur.* **2020**, *2020*, 8. [CrossRef]
81. Ksibi, S.; Jaidi, F.; Bouhoula, A. Cyber-Risk Management within IoMT: A Context-Aware Agent-Based Framework for a Reliable e-Health System. In Proceedings of the 23rd International Conference on Information Integration and Web Intelligence, Linz, Austria, 29 November–1 December 2021; pp. 547–552.
82. Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. Digital Healthcare-Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. *IEEE Access* **2022**, *10*, 12345–12364. [CrossRef]
83. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Trans. Comput. Healthc.* **2021**, *2*, 1–44. [CrossRef]
84. Gressl, L.; Krisper, M.; Steger, C.; Neffe, U. Towards Security Attack and Risk Assessment during Early System Design. In Proceedings of the IEEE 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland, 15–19 June 2020; pp. 1–8.
85. Mohsin, M.; Sardar, M.U.; Hasan, O.; Anwar, Z. IoTRiskAnalyzer: A probabilistic model checking based framework for formal risk analytics of the Internet of Things. *IEEE Access* **2017**, *5*, 5494–5505. [CrossRef]
86. Pal, D.; Funilkul, S.; Charoenkitkarn, N.; Kanthamanon, P. Internet-of-things and smart homes for elderly healthcare: An end user perspective. *IEEE Access* **2018**, *6*, 10483–10496. [CrossRef]
87. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cybersecurity. *Technol. Innov. Manag. Rev.* **2014**, *4*, 13–21. [CrossRef]
88. Lu, Y.; Da Xu, L. Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet Things J.* **2018**, *6*, 2103–2115. [CrossRef]
89. Ginter, P.M.; Duncan, W.J.; Swayne, L.E. *The Strategic Management of Health Care Organizations*; John Wiley & Sons: Hoboken, NJ, USA, 2018.
90. Angst, C.M.; Block, E.S.; D'Arcy, J.; Kelley, K. When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *Mis Q.* **2017**, *41*, 893–A8. [CrossRef]
91. Xu, S.; Yung, M.; Wang, J. Seeking Foundations for the Science of Cyber Security: Editorial for Special Issue of Information Systems Frontiers. *Inf. Syst. Front.* **2021**, *23*, 263–267. [CrossRef]
92. Tweneboah-Koduah, S.; Skouby, K.E.; Tadayoni, R. Cyber security threats to IoT applications and service domains. *Wirel. Pers. Commun.* **2017**, *95*, 169–185. [CrossRef]
93. *ANSI/AAMI/ISO 14971: 2007/(R) 2010*; Medical Devices—Application of Risk Management to Medical Devices. AAMI: Melbourne, Australia, 2007.
94. Mansfield-Devine, S. DevOps: Finding room for security. *Netw. Secur.* **2018**, *2018*, 15–20. [CrossRef]
95. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]

96. Sicari, S.; Rizzardi, A.; Miorandi, D.; Coen-Porisini, A. A risk assessment methodology for the Internet of Things. *Comput. Commun.* **2018**, *129*, 67–79. [CrossRef]
97. Abie, H.; Balasingham, I. Risk-based adaptive security for smart IoT in eHealth. In Proceedings of the 7th International Conference on Body Area Networks, Oslo, Norway, 24–26 February 2012; pp. 269–275.
98. Jacobs, V.; Bulters, J.; van Wieren, M.; Koch, R.; Rodosek, G. Modeling the impact of cyber risk for major Dutch organizations. In Proceedings of the Deloitte Cyber Risk Services, European Conference on Cyber Warfare and Security, 2016; pp. 145–154.
99. Sieber, D.A.; Adams, W.P., Jr. What's your micromort? A patient-oriented analysis of breast implant-associated anaplastic large cell lymphoma (BIA-ALCL). *Aesthetic Surg. J.* **2017**, *37*, 887–891. [CrossRef]
100. Matheu-García, S.N.; Hernández-Ramos, J.L.; Skarmeta, A.F.; Baldini, G. Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Comput. Stand. Interfaces* **2019**, *62*, 64–83. [CrossRef]
101. Ge, M.; Hong, J.B.; Guttmann, W.; Kim, D.S. A framework for automating security analysis of the internet of things. *J. Netw. Comput. Appl.* **2017**, *83*, 12–27. [CrossRef]
102. Duan, X.; Ge, M.; Le, T.H.M.; Ullah, F.; Gao, S.; Lu, X.; Babar, M.A. Automated security assessment for the internet of things. In Proceedings of the 2021 IEEE 26th Pacific Rim International Symposium on Dependable Computing (PRDC), Perth, Australia, 1–4 December 2021; pp. 47–56.
103. Stiawan, D.; Idris, M.; Malik, R.F.; Nurmaini, S.; Alsharif, N.; Budiarto, R. Investigating brute force attack patterns in IoT network. *J. Electr. Comput. Eng.* **2019**, *2019*, 4568368 . [CrossRef]
104. Mughal, A.A. Building and Securing the Modern Security Operations Center (SOC). *Int. J. Bus. Intell. Big Data Anal.* **2022**, *5*, 1–15.
105. Jalali, M.S.; Kaiser, J.P. Cybersecurity in hospitals: A systematic, organizational perspective. *J. Med. Internet Res.* **2018**, *20*, e10059. [CrossRef]
106. Zhang, G.; Navimipour, N.J. A comprehensive and systematic review of the IoT-based medical management systems: Applications, techniques, trends and open issues. *Sustain. Cities Soc.* **2022**, *82*, 103914. [CrossRef]
107. Riesco, R.; Villagrá, V.A. Leveraging cyber threat intelligence for a dynamic risk framework: Automation by using a semantic reasoner and a new combination of standards (STIX™, SWRL and OWL). *Int. J. Inf. Secur.* **2019**, *18*, 715–739. [CrossRef]
108. Antonello, F.; Buongiorno, J.; Zio, E. A methodology to perform dynamic risk assessment using system theory and modeling and simulation: Application to nuclear batteries. *Reliab. Eng. Syst. Saf.* **2022**, *228*, 108769. [CrossRef]
109. Collen, A.; Szanto, I.C.; Benyahya, M.; Genge, B.; Nijdam, N.A. Integrating Human Factors in the Visualisation of Usable Transparency for Dynamic Risk Assessment. *Information* **2022**, *13*, 340. [CrossRef]
110. Moustafa, N.; Adi, E.; Turnbull, B.; Hu, J. A new threat intelligence scheme for safeguarding industry 4.0 systems. *IEEE Access* **2018**, *6*, 32910–32924. [CrossRef]
111. Czekster, R.M. Leveraging Cyber Threat Intelligence in Smart Devices. In *Information Security and Privacy in Smart Devices: Tools, Methods, and Applications*; IGI Global: Hershey, PA, USA, 2023; pp. 71–95.
112. Bolhasani, H.; Mohseni, M.; Rahmani, A.M. Deep learning applications for IoT in health care: A systematic review. *Inform. Med. Unlocked* **2021**, *23*, 100550. [CrossRef]
113. Panch, T.; Szolovits, P.; Atun, R. Artificial intelligence, machine learning and health systems. *J. Glob. Health* **2018**, *8*, 020303. [CrossRef] [PubMed]
114. Lee, D.; Yoon, S.N. Application of artificial intelligence-based technologies in the healthcare industry: Opportunities and challenges. *Int. J. Environ. Res. Public Health* **2021**, *18*, 271. [CrossRef] [PubMed]
115. Manne, R.; Kantheti, S.C. Application of artificial intelligence in healthcare: Chances and challenges. *Curr. J. Appl. Sci. Technol.* **2021**, *40*, 78–89. [CrossRef]
116. Jamal, A.A.; Majid, A.A.M.; Konev, A.; Kosachenko, T.; Shelupanov, A. A review on security analysis of cyber physical systems using Machine learning. *Mater. Today Proc.* **2023**, *80*, 2302–2306. [CrossRef]
117. Mukati, N.; Namdev, N.; Dilip, R.; Hemalatha, N.; Dhiman, V.; Sahu, B. Healthcare assistance to COVID-19 patient using internet of things (IoT) enabled technologies. *Mater. Today Proc.* **2023**, *80*, 3777–3781. [CrossRef]
118. Quy, V.K.; Hau, N.V.; Anh, D.V.; Ngoc, L.A. Smart healthcare IoT applications based on fog computing: architecture, applications and challenges. *Complex Intell. Syst.* **2022**, *8*, 3805–3815. [CrossRef] [PubMed]
119. Balasamy, K.; Krishnaraj, N.; Ramprasath, J.; Ramprakash, P. A secure framework for protecting clinical data in medical IoT environment. In *Smart Healthcare System Design: Security and Privacy Aspects*; Wiley: Hoboken, NJ, USA, 2022; pp. 203–234.
120. Bruynseels, K.; Santoni de Sio, F.; Van den Hoven, J. Digital twins in health care: Ethical implications of an emerging engineering paradigm. *Front. Genet.* **2018**, *9*, 31. [CrossRef]
121. Ahmadi-Assalemi, G.; Al-Khateeb, H.; Maple, C.; Epiphaniou, G.; Alhaboby, Z.A.; Alkaabi, S.; Alhaboby, D. Digital twins for precision healthcare. In *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*; Springer: Cham, Switzerland, 2020; pp. 133–158.
122. Laamarti, F.; Badawi, H.F.; Ding, Y.; Arafsha, F.; Hafidh, B.; El Saddik, A. An ISO/IEEE 11073 standardized digital twin framework for health and well-being in smart cities. *IEEE Access* **2020**, *8*, 105950–105961. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.