IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 16, 2020, accepted February 15, 2021, date of publication March 9, 2021, date of current version March 17, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3064682

Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal

VANGELIS MALAMAS, (Graduate Student Member, IEEE), FOTIS CHANTZIS, THOMAS K. DASAKLIS, GEORGE STERGIOPOULOS, (Member, IEEE), PANAYIOTIS KOTZANIKOLAOU, (Member, IEEE), AND CHRISTOS DOULIGERIS, (Senior Member, IEEE)
Department of Informatics, University of Piraeus, 185 34 Piraeus, Greece

Corresponding author: Vangelis Malamas (bagmalamas@unipi.gr)

This work was supported by the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation, under the call RESEARCH–CREATE–INNOVATE under Project T1EDK-01958.

ABSTRACT The Internet of Medical Things (IoMT) has revolutionized health care services by providing significant benefits in terms of patient well being and relevant costs. Traditional risk assessment methodologies, however, cannot be effectively applied in the IoMT context since IoMT devices form part of a distributed and trustless environment and naturally support functionalities that favor reliability and usability instead of security. In this work we present a survey of risk assessment and mitigation methodologies for IoMT. For conducting the survey, we assess two streams of literature. First, we systematically review and classify the current scientific research in IoMT risk assessment methodologies. Second, we review existing standards/best practices for IoMT security assessment and mitigation in order to i) provide a comparative assessment of these standards/best practices on the basis of predefined criteria (scope and/or coverage, maturity level, and relevant risk methodology applied) and ii) identify common themes for IoMT security controls. Based on the analysis, we provide various IoMT research and implementation gaps along with a road map of fruitful areas for future research. The paper could be of significant value to security assessment researchers and policymakers/stakeholders in the health care industry.

INDEX TERMS Internet of Medical Things, medical device security, risk assessment, threat modeling, vulnerability assessment, impact assessment.

I. INTRODUCTION

The Internet of Medical Things (IoMT) consists of high-risk, high-value devices which are placed and inter-connected to hospital and other healthcare networks. According to the US Food Drug & Cosmetic Act a medical device is defined as an instrument intended for use in the "diagnosis, cure, mitigation, treatment, or prevention of disease" [1]. An *inter-connected* medical device (or IoMT device) is performing the generation, collection, analysis of a patient medical data along with the transmission of those data. Regarding the transmission, through the healthcare provider networks, an IoMT device transmits information (e.g. health or technical data) either to the cloud or to internal servers in order to monitor a patient's health parameters and help prevent, diagnose or treat diseases. According to [2], more than 3.7 million connected medical devices are in use, for monitoring vital physiologic parameters of patients, thus improving healthcare decision-making. Recent reports predict an exponential growth of the IoMT market worldwide, up to $136.8 billion by 2021, according to Allied Market Research [3]. This is underlined by the fact that the healthcare system will increase its needs as the population continues to age.

However, due to their increased inter-connectivity, IoMT devices may serve as an attack surface for various threat actors targeting against sensitive health data or systems. For example, taking into account real attack scenarios in IoMT [4], malicious actors may compromise sensitive data such as Patient Health Information (PHI) [5] and medical research intellectual property [6], or use IoMT devices as a

The associate editor coordinating the review of this manuscript and approving it for publication was Zheng Yan.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

means to cause direct patient harm [7]. The cybersecurity vulnerabilities that affect IoMT devices may be similar to any other networked device but their impact can be far more detrimental [8]. In addition, IoMT devices are usually implemented in a distributed and trustless environment and are responsible for supporting several functionalities in various physical locations, thus issues of IoMT security are becoming increasingly acute nowadays.

*Classification of IoMT devices.*There are several classifications regarding medical devices. Some of them focus on device functionality or contain typical non-connected medical devices, like GMDN's classification [9]. In [10], the authors present a classification, which includes only interconnected medical devices placing them into four main categories:

- **Physiologic monitoring:** Devices that are used for monitoring signals passively from the patient's body such as *wearable* and *indigestible* devices.
- **Medical treatment:** Devices that are actively participate in the patient treatment, such as *implantable medical devices* (IMD) and *infusion pumps*.
- **In-hospital connected:** Devices that are placed inside a hospital environment and could be *institutional medical devices* or *Surgical Robotics*.
- **Ambient:** Devices supporting assisting treatment processes, such as *patient identification*, *movement detection*, *sensors* etc.

In another classification, the US Food and Drug Association (FDA) segregates medical devices in three main categories. Classification criteria synthesizes medical device's complexity and the *medical risk* involved during the usage phase [11]. In particular, Class I contains those medical devices that are subject to the lowest risk level. These devices are expected to comply with the lowest level of regulatory controls. Class II, on the other hand, contains devices with more complexity comparing to those of level I. This second level of classification includes devices that are considered to have higher risk level than Class I devices. The higher the risk the more forceful regulatory controls are in order to provide assurance of their effectiveness. In Class III the most complex medical devices are included. The high complexity implies highest risk, and therefore, entail more stringent regulatory controls. For example an implantable pacemakers is a Class III device, since a malfunction or a deliberate attack against it could result to fatal impact for the patient. Note that the categorization provided by the US FDA does not differentiate connected devices (IoMT) from non-connected devices.

Security, privacy and safety requirements for IoMT. Protecting healthcare systems from cyber-threats is a challenging task that requires balancing security and privacy goals, with patient safety and utility. Since patient safety always remains the top priority, the security controls should be carefully selected to prevent healthcare service unavailability or disruptions that could compromise the patients' health and well-being. According to recommendations issued by the FDA [12], [13] and the MDS2 [14] and EU MDR [15] procurement guidelines, medical devices should satisfy various security and privacy requirements. From a security perspective, IoMT devices should i) support authentication and fine-grained access control, ii) allow access to devices by trusted users only, iii) guarantee medical data integrity and confidentiality and code execution integrity, iv) prevent malicious alteration or execution of critical device functionalities and device availability, and v) protect from Denial-of-Service (DoS) attacks. From a privacy point of view, IoMT devices should i) support device-existence and device-type privacy, so as to prevent unauthorized entities from being aware of the existence (or type) of the device, ii) serve as a strong privacy guarantee by protecting logs and telemetry information from privacy breaches as well as by protecting private medical information from disclosure. At the same time, IoMT devices should also satisfy safety and utility prerequisites [16] related to device configurability and audibility, resource efficiency and multi-device coordination.

A. MOTIVATION AND CONTRIBUTION

Various security aspects relevant to IoT (Internet of Things) applications are gaining significant attention in nowadays [17]–[23]. In particular, several authors cover the security aspects of various IoT frameworks [24], [25] and relevant security issues of IoT architectures [4], [26], [27] and communication protocols [28]. Some studies have also highlighted the importance of properly defining security requirements for IoT applications [29], [30].

Special attention has also been paid in Internet of Medical Things applications [31]–[33] particularly on security issues for implantable medical devices [34], [35]. Three surveys closest to our work can be found in [36] and [37] and [38]. The first [36] covers specific areas of security and privacy by providing an in depth analysis of IoMT data collection and management. The second [37] and the third [38] review papers have a wider scope. They provide a survey of security vulnerabilities, recent attacks and possible countermeasures for IoMT devices. However, none of the above surveys examine risk assessment and mitigation methodologies for IoMT devices. In fact, as discussed in the literature, [4], [37], traditional risk assessment methodologies cannot always capture the new threat landscape generated by the integration of IoT systems in critical sectors such as energy, healthcare and industrial control. As each sector is affected by different threat agents, it is not possible to compare methodologies targeted to different critical sectors. Therefore, a comprehensive appraisal of the various risk assessment methodologies and relevant security controls for IoMT devices is still missing from the literature.

Table 1 summarizes the various features and scope of the relevant health-oriented IoT surveys as well as the scope/purpose of our survey.

Our motivation in this work is to cover the aforementioned gap in the literature by providing a comprehensive and structured appraisal of the various risk assessment methodologies

TABLE 1. Related survey papers.

Reference	Topic	Purpose
[32]	Smart health and surveillance	Security and protection issues of health-oriented IoT applications with a focus on smart health care services.
[33]	Security issues of Near Field Communication (NFC) and Radio Frequency Identification (RFID) used in e-Health applications	Security challenges attributed to the multiple standards used for NFC readers and RFID tags.
[31]	Generic health care applications	Aspects of multi-factor authentication, different types of security attacks, risk and security gaps in healthcare systems.
[37]	IoMT	Identification of vulnerabilities and attacks along with possible mitigation measures, and regulations for IoMT devices.
[34]	Implantable medical devices	Identification of the main security goals of implantable medical devices and relevant protection mechanisms.
[35]	Implantable medical devices	Challenges and constraints associated with securing implantable medical devices, particularly in emergency situations and resource-constraint contexts.
[36]	IoMT	Security and privacy of IoMT-related health data.
[38]	IoT	Classification of IoT risk assessment methodologies with a specific focus on SCADA, financial and healthcare systems.
Our survey	IoMT	Classification of IoMT risk assessment methodologies and identification of IoMT-specific security controls (both scientific and grey literature). Identification of research and implementation gaps.

and security controls for the IoMT. In summary, our main contributions are:

- Concerning the scientific literature, since the scope of the survey is risk assessment methodologies for IoMT, we have structured our taxonomy based on the three main processes of risk assessment, that is Threat, Vulnerability and Impact assessment. For each phase we examine/compare the main approaches (e.g. for threat assessment we examine what threat models have been proposed for IoMT, what types of threats they cover etc). In addition, we identify common threats and vulnerabilities in the IoMT security domain.
- Concerning the grey literature (standards, best practices and guidelines), related to IoMT security, we provide a detailed set of criteria containing the coverage of each standard (e.g. what phases of RA they cover), their risk methodology and their maturity.
- Based on the analysis preformed in previous steps we identify relevant research gaps and future research suggestions for research in RA and RM methodologies for IoMT and the health sector.
- Finally, concerning risk mitigation, we provide a list of security controls that can be used for risk mitigation in IoMT and we document this list based on the study of both streams of literature (scientific and gray). We further elaborate on their effectiveness and contribution to protecting IoMT devices.

B. STRUCTURE OF THE SURVEY

In Section II we provide the methodological approach adopted for conducting our systematic survey. In Section III, we present a classification of the available scientific literature while in Section IV we provide a classification and comparative appraisal of various standards and best practices related to IoMT security assessment and mitigation. In Section V, we aggregate and present the most common security controls pertaining to relevant IoMT security standards and best practices. In Section VI we present a comprehensive and structured synthesis of the various research and implementation gaps as derived from our previous analysis and we further highlight fruitful future research areas. The paper ends with some concluding remarks.

II. RESEARCH METHODOLOGY

For providing a transparent, reproducible and sound overview of the scientific literature regarding IoMT risk assessment methodologies, we made use of the process suggested by [39] along with certain features of the PRISMA statement [40]. Our overall methodological approach includes the following four steps:

1) Planning the survey (needs identification and development of the survey protocol).
2) Searching (identification of the selected studies based on targeted searches).
3) Screening (studies' selection and quality appraisal).
4) Synthesis and reporting (extraction of the available data, synthesis of the main findings and reporting of the results).

A. RESEARCH OBJECTIVES AND SEARCH STRATEGY

The overall survey process starts by defining which research questions are in scope, in order to better understand the

TABLE 2. Research questions and objectives of the survey.

Research questions	Objectives
RQ1: What approaches are proposed in the scientific literature to support decision processes for IoMT risk assessment?	The intention here is to provide a systematic classification of the available risk assessment frameworks presented in the scientific literature.
RQ2: What are the common key criteria related to IoMT risk assessment as derived from relevant standards and best practices?	The objective here is twofold. First, to derive common criteria prevalent to standards and best practices related to IoMT risk assessment. Second, based on these criteria to present a comparative appraisal and classification of the available standards and best practices.
RQ3: What are the IoMT specific security controls that could be derived from the available literature?	Since traditional risk assessment methodologies cannot be effectively applied in the context of IoMT devices, the objective here is to derive key IoMT security controls. Therefore, based on both streams of literature (scientific and grey) the aim is to present a synthesis of IoMT-specific security controls.
RQ4: What are the current research gaps related to risk assessment methodologies for IoMT devices?	The aim here is to provide a structured analysis related to both research and implementation gaps and futher highlight the interrelationships between these gaps and relevant IoMT security controls.

TABLE 3. Key words used during the search phase.

Scientific literature	Grey literature
ABS (IoMT OR "Internet of Medical Things" OR IoT OR "Internet of Things" OR "medical IoT" OR MIoT OR "IoT healthcare" AND "risk assessment" OR "vulnerability assessment" OR "threat modeling" OR "threat models" OR "threat assessment" OR "impact assessment" OR vulnerability OR threat OR impact AND (risk AND security))	Medical devices, security, risk assessment

available risk assessment methodologies and security controls for IoMT devices. In addition, they help us derive the various IoMT research and implementation gaps and further provide areas for future research. Selected research questions and relevant objectives are presented in Table 2.

For conducting our survey and addressing our research questions, we carried out a systematic literature search during October 2020 without time-frame restrictions. Scopus and Google were used as the main search engines. In particular, Scopus was used for retrieving all the scientific-related literature whereas Google was used for locating relevant standards and best practices (grey literature). A predefined set of keywords were used for searching in both search engines (Table 3). It is worth noting that the first, bulk search query in Scopus returned 1566 results. Various refinement features of the Scopus database were extensively applied (fine-tuning of results in accordance with the context of specific articles, relevant papers, subject area etc).

Based on the assessment of the first 200 hits from Google, we identified the available grey literature. We did not include more Google results because beyond a certain point: a) Google query returned a lot of irrelevant results of rather poor quality and minor impact (as stated in our exclusion criteria list) b) not all actual results were visible and accessible (many hyperlinks were broken or inactive). It should be noted that Google searches were used as a supplementary search strategy (particularly for streamlining the assessment) and our primary source for locating studies was Scopus. Besides, the total number of documents retrieved from Google was relatively low compared to the bibliography retrieved from Scopus.

The identification of additional studies took place by using the so-called snowball effect by which references of key articles/reports were searched for identifying additional citations. For all the potentially relevant articles and reports we managed to locate the full texts. It is worth noting that the hand-search reference gathered from various articles helped us retrieve additional grey literature sources like committee reports and/or policy briefs from institutions/organizations like the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), The Open Web Application Security Project (OWASP), the Mayo clinic and the European Union Agency for Cybersecurity (ENISA).

B. SELECTION OF STUDIES AND ANALYSIS

For assessing the eligibility of the retrieved literature (scientific and grey) we used various pre-defined exclusion and inclusion criteria (listed in Table 4). For narrowing down the number of papers retrieved we applied some exclusion

TABLE 4. Selection criteria.

Selection criteria	Scientific database		Grey literature
Inclusion	Peer-reviewed scientific research papers (including articles in press), book chapters, conference proceedings papers, review papers, serials etc.		Industry reports, committee reports, policy briefs (written in English)
	Without time-frame restrictions		Without time-frame restrictions
Exclusion	Before importation to the bibliographic manager	Non English-written papers or papers with missing abstracts.	Generic reports relevant to security and/or privacy aspects of IoMT devices without describing specific risk assessment methodological frameworks.
	During title screening	IoT-related articles relevant to security and/or privacy aspects of connected devices.	
	During abstract screening	IoT-related articles relevant to security and/or privacy aspects of medical devices.	
	During full-text reading	IoMT articles describing no specific risk assessment methodological frameworks.	

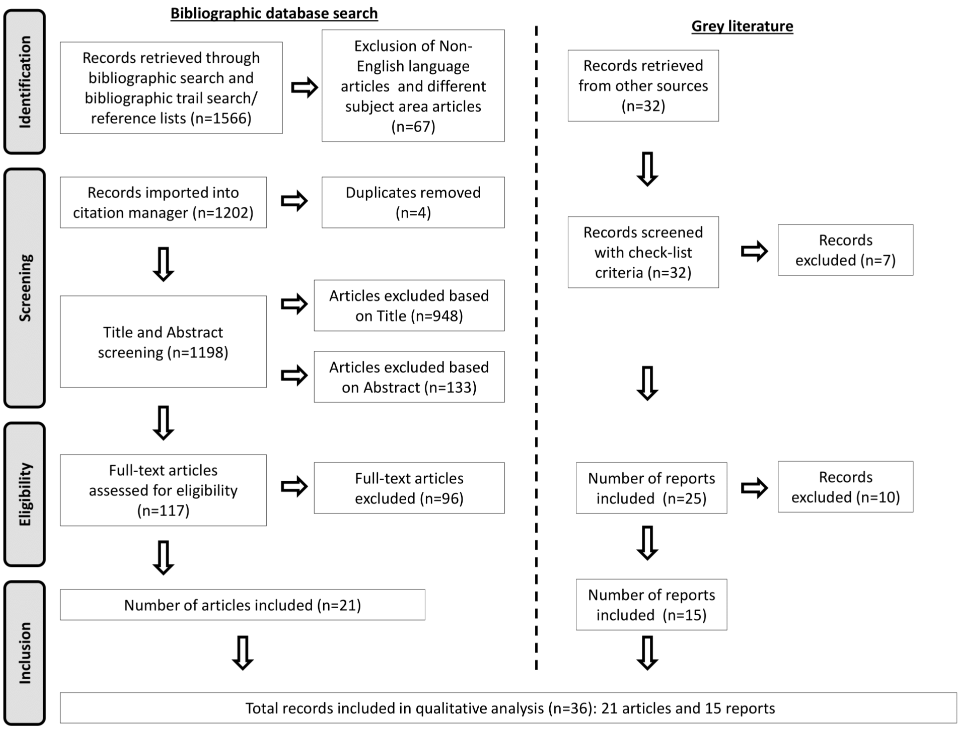

Bibliographic database search
Grey literature
Identification
Screening
Eligibility
Inclusion
Records retrieved through bibliographic search and bibliographic trail search/ reference lists (n=1566)
Exclusion of Non-English language articles and different subject area articles (n=67)
Records retrieved from other sources (n=32)
Records imported into citation manager (n=1202)
Duplicates removed (n=4)
Records screened with check-list criteria (n=32)
Records excluded (n=7)
Articles excluded based on Title (n=948)
Title and Abstract screening (n=1198)
Articles excluded based on Abstract (n=133)
Full-text articles assessed for eligibility (n=117)
Full-text articles excluded (n=96)
Number of reports included (n=25)
Records excluded (n=10)
Number of articles included (n=21)
Number of reports included (n=15)
Total records included in qualitative analysis (n=36): 21 articles and 15 reports

FIGURE 1. Flowchart of the search strategy.

criteria prior to importing the retrieved literature in the reference manager software (restrictions related to document type, language and subject area). The overall selection process consisted of the following steps: a) the titles of all scientific articles and reports were assessed for relevance. Articles and/or reports which met one of the exclusion criteria were excluded from the analysis and were sorted by reason of exclusion b) all the paper abstracts and introduction sections of reports (grey literature) were assessed for relevance. Articles and/or reports that met one of the exclusion criteria defined were excluded from the analysis and we documented the reason of exclusion c) We also conducted a full-text reading and some additional articles/reports were excluded during this step and were sorted by reason of exclusion. Any possible discrepancy among authors regarding the relevance of the retrieved articles/reports was resolved through discussion until unanimous agreement was reached.

We made use of a qualitative analysis software (MAXQDA11) for analyzing (in emerging themes) all the articles and/or reports which met the inclusion criteria. The thematic content analysis was independently carried out by the authors. Various qualitative analysis methods (i.e., narrative synthesis and thematic analysis) were used for the

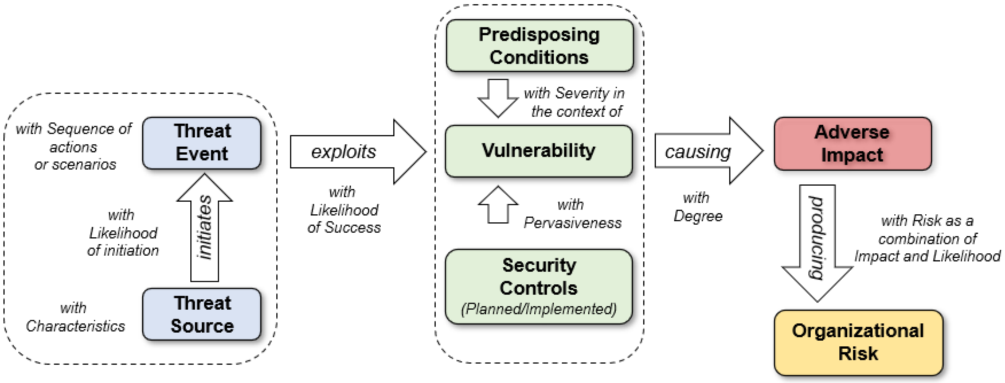

with Sequence of actions or scenarios
Threat Event
initiates
with Likelihood of initiation
with Characteristics
Threat Source
exploits
with Likelihood of Success
Predisposing Conditions
with Severity in the context of
Vulnerability
with Pervasiveness
Security Controls (Planned/Implemented)
causing
with Degree
Adverse Impact
producing
with Risk as a combination of Impact and Likelihood
Organizational Risk

FIGURE 2. Generic Risk model.

classification and synthesis of the extracted data. We report the results of our analysis in Sections III and IV.

III. CLASSIFICATION OF THE IoMT SECURITY ASSESSMENT METHODOLOGIES

In this section we analyze the scientific literature for the security assessment of medical devices as identified using the research methodology described in Section II. In cybersecurity, risk assessment is a multi-process approach that involves various phases; identifying and assess relevant security threats, analysis of the underlying vulnerabilities of the system under examination, and analysis of the consequences (or impact) of potential security loss [41]. To assist the reader, first we describe the terminology and the main phases of a risk assessment and, then, we classify the relevant bibliography[1] according to these phases. We analyze the existing research works by examining their main characteristics, similarities and differences. Based on this, we identify the relevant research gaps (discussed separately in Section VI).

A. SECURITY ASSESSMENT: A GENERIC RISK MODEL

The IoMT security assessment is evaluated based on standardized information security management practices. Information security management follows a *risk-based* approach: by assessing the potential security risks (i.e. the combined effect of a potential security event and its relative consequences) against a system under examination, it is easier to manage and mitigate potential sources of security events (aka threats), identify and reduce the exposure (aka vulnerabilities) against security breaches and/or limit the consequences (aka impact) of successful security breaches. Well-known security standards, such as those published by NIST [42]–[44] and ISO [45] generally define risk assessment as a holistic process of identifying risks, analyze and evaluate them, through a combination of various input from different security assessment sub-processes, such as threat, vulnerability and impact assessment. The output of the risk assessment phase is taken as input for the risk mitigation phase. A generic risk model based on [46] is shown in Fig. 2.

Threat assessment is a procedure where the identification and evaluation of entities and actions (either natural or human-made) is being performed that could potentially have a negative effect on life, information, operations and property. For example events which could adversely affect assets or operations of the examined system/organization [47]. A security threat may violate one or more security properties such as confidentiality, integrity and availability of data, systems and services.

Vulnerability assessment is a method that aims to identify technical and/or non-technical weaknesses of assets or services, that may be exploited by threat agents with the scope of defining a potential security threat. Asset vulnerabilities and potential threats are mapped in a many-to-many relation.

Impact assessment is a method that aims to identify the consequences of a potential security violation. A way to assess the impact of security loss is to examine the worst-case consequences of potential security losses. For example, if the unavailability of a critical medical system for a couple of hours could lead to fatal results – in the worst-case scenario – then the unavailability impact for this system would be very high. Similarly, if the disclosure (loss of confidentiality) of a medical database could lead to severe regulatory/legal penalties, then again the disclosure impact for this asset would be high.

Finally, *risk mitigation* or *risk treatment* builds upon the results from the previous Risk assessment phase, and includes all actions and changes that are deemed necessary according to the scope, the organisation's strategy and decisions delegated to responsible parties during the Risk Assessment phase [45], [60]. Such risk mitigation strategies reflect the organisation's cybersecurity needs and identify all necessary actions "to reduce information security risks to organizational operations and assets" [60]. These actions involve a combination of risk response measures across the three categories of changes: (i) Use and update of common security controls,

[1] Note that some research works may deal with more than one risk assessment process.

(ii) re-modeling of the business or everyday processes inside an organisation, and (iii) the implementation of new operational, or technical safeguards or countermeasures. Implementation of risk mitigation measures is often supported by assurance processes that involve measuring the compliance of all changes made in light of the newly identified needs of the organization (e.g. by testing the configuration of newly installed firewalls as measure for mitigating risk over a network).

B. THREAT ASSESSMENT FOR IoMT DEVICES

During the threat assessment phase, the likelihood of potential security threats is assessed. Since cyber-security threats are usually human-made and may not attributed to natural events, it is not easy to have credible statistics. A common way to identify cyber-security threats is to apply threat modeling (see for example [43], [61]). In particular, to prevent threats from taking advantage of system flaws, experts often use threat models to create an abstraction of the system, profile potential malicious actors including their motivation, methods and available resources and construct a catalog of potential threats. Various works describe different approaches for modelling and assessing threats; usually based on an existing widely accepted methodology. For example, in [61] the most commonly used methodologies are presented and a comparison is made among them for establishing the suitability of each methodology based on particular features.

a: THREAT MODELING FOR IoMT

Several studies exist that address issues of threat modeling for IoT and IoMT devices. For example, in [4] threats against IoT devices are grouped based on: (i) the *required access* to the IoT device; (ii) the *required capabilities* and (iii) the *required motivation* of the adversary. The threat model, which is based in attack paths, examines how the likelihood is shaped depending on the adversary's access level, capabilities and motivation. The paper, which is not based in any of the well-known methodologies, defines a metric scale for calculating the threat level. An important finding is that all the adversaries for the IoMT paradigm need to be strongly motivated. Other studies classify the threat agents in a different way. For instance, in [56], methodology is based on adversarial model. The authors identify two types of attackers in IoT health systems: a) Internal Attackers (that exist within the healthcare system and execute malicious operations secretly), and b) External Attackers (that reside outside the healthcare system and perform malicious activities. An adversarial model is also presented in [57], combined with an asset-based approach. The authors identify key assets (personal, physical, information, and intangible assets) and they further classify the vulnerabilities that can be exploited by a threat agent to harm a system. In [48], a threat model that is specifically targeted to medical cyber-physical systems is presented with qualitative metrics. The proposed model separates the users into trustworthy, trusted but error-prone, untrustworthy and temporarily trustworthy. The paper also defines adversary's motivation to breach privacy or direct influence patient's health. In another work [50], an adversarial threat model against mobile health systems, including IoMT, are examined and classified using the STRIDE [61] methodology which recognizes as threat categories the following: Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and elevation of privileges. The threat ranking, which is based on the DREAD model [61], takes into account the Damage potential, Reproducibility, Exploitability, Affected users and Discoverability. The threat sources are described along with the adversary's capabilities. Other studies build upon the CIA triad and the Microsoft STRIDE frameworks for developing innovative threat assessment frameworks for identifying the parts of the system that need to be better secured for Consumer Health Wearables (CHW) [55], which is a subgroup of IoMT devices. In [52], several threats linked to short or long range mobile wireless communication infrastructures are identified with a particular focus on applications that employ such types of infrastructure (e.g. biomedical sensor networks).

An important aspect of threat modeling relates to the prioritization and categorization of the various threats. For example, in [54], an attack-tree approach is presented, where a broad range of interdependent threats is analyzed based on a Multiple-Valued Logic in order to establish the status of a large-scaled system along with a multiple-valued decision diagram for indexing and analyzing the threats. The objective is to catalogue the various threats based on common features. A mechanism for prioritising IoMT threats is presented in [51]. The proposed mechanism, based on the UK HMG IS11 approach, is further tested using the Technology Integrated Health Management test-bed, introducing customized qualitative metrics. Other studies categorize the various threats based on the type of the likely intruders and their capabilities. For example, in [49] threats are identified based on the capabilities (skills and resources needed to perform attacks) of the attackers (individual attacker, organized groups and state-sponsored actors) and are then linked with measurable weights. In [53], various Bluetooth security threats are grouped into three categories that include disclosure, integrity and denial of service. A system-theoretic process analysis (STPA) approach is presented in [58] applied to specific medical devices such as insulin pumps. The authors make use of attack-tree structure analysis as part of their threat analysis model. In [59] The authors use a threat-oriented analytical approach to split the analysis into three parts, an actor-based analysis to assess the effects of the attacks, a scenario-based analysis to calculate the possibility of threats happening, and a composite analysis to classify the most dangerous attack findings. Table 5 presents a comparison of the various IoMT threat models found in the scientific literature. The assessment is based on key criteria pertaining to the various threat modeling approaches. These criteria include the motivation and the capabilities assumed for the adversary along with the threat sources identified.

TABLE 5. A comparison of IoMT threat models found in the literature.

Literature	Relevant standards	Threat identification	Threat assessment	Adversarial capabilities
[4]	NIST SP 800-30	Attack-paths	QT	Low to High
[48]	n/a	Adversarial model	QT	n/a
[49]	n/a	Adversarial model	QT	Low to High
[50]	n/a	STRIDE/DREAD	QL	Medium to High
[51]	ISO 27033	HMG IS1	QL	Low to High
[52]	n/a	Adversarial model	n/a	Low to High
[53]	n/a	Attack-paths	QL	High
[54]	n/a	Logic Decision Diagram	QT	n/a
[55]	ISO 27001	STRIDE	QL	n/a
[56]	n/a	Adversarial model	QL	High
[57]	n/a	Asset-based	QL	n/a
[58]	STPA	Attack/Defense tree	QT	n/a
[59]	NIST SP 800-30	Adversarial model	QT	High

*QL = Qualitative scale used , QT = Quantitative (number) scale used.

TABLE 6. Common threats against IoMT.

Category	Threat	Threat description
Spoofing	User impersonation	impersonation of physician, nurse, device operator, administrator of healthcare systems
	Device impersonation	node cloning, setting up rogue medical devices or components for example, a malicious drug library server that communicates with a drug infusion pump
Tampering	Patient data tampering	malicious altering of patient information
	Malicious input	includes attacks like SQL injection and XSS
	Communication modification	malicious altering of data in transit
	Device failure	device malfunction, potentially affecting patient care
	Device tampering	altering of device settings, installation of backdoors
	Replay attack	valid transmission is maliciously replayed to victim
Repudiation	Log deletion	removal of system / debugging logs with the intent of covering attacker's tracks or for repudiation
	Data delivery	medical information manipulation in the name of other patients
Information Disclosure	Medical information disclosure	exposure of protected health information
	Data eavesdropping	capturing of communication data
	Side-channel attack	inference of sensitive info using timing or power consumption data
	IMD type determination	identify type of implantable device
	IMD tracking	determining the device ID and tracking individual IMDs
Denial of Service	Battery Drain attack	causing the battery life to rapidly decrease by preventing the device from going to sleep or energy saving mode
	Signal jamming	cause interference to wireless communication of legitimate endpoints
	Flooding	continuously sending messages to cause a Denial of Service
Elevation of Privilege	Maintenance compromise	remote support connection from medical device vendor's network is compromised and used to access the medical device with elevated privileges
	Insecure API	exposed API allows unauthenticated adversaries to conduct high-privileged actions on device

b: COMMON THREATS AGAINST IoMT

Based on the review of the literature presented above, the threat identification and assessment for IoMT usually relies on the STRIDE threat model [50], [55] or variations of it [49], [52]. In Table 6, we summarize some of the most common threats against IoMT, as identified in the literature, and categorized using the STRIDE model. Notably, many of these threats overlap with threats identified in other IoT ecosystems [62]. Due to the IoMT hardware limitations (e.g. battery constraints) some mitigation mechanisms are hard or impossible to be implemented and therefore these devices have a much wider threat coverage.

All of the threats presented in Table 6 can lead to critical exposure of the patients health, causing even fatal impact.

For example threats related to spoofing or tampering like, for instance, device impersonation, malicious input and device tampering, could allow an adversary to alter drug dosage for specific patients or extract sensitive information. Furthermore depending on the type of IoMT device, Denial of Service (DoS) attacks could be lethal (e.g implantable devices). In Section V we will also examine the mitigation security controls proposed in the literature, with respect to those security threats.

C. VULNERABILITY ASSESSMENT FOR IoMT

The scope of a vulnerability assessment is to identify technical and/or non-technical security flaws which could be exploited by malicious users to realize a security threat. The term ''vulnerability assessment'' is used here in the broader sense which involves not only automated vulnerability scanning but also manual security testing. Vulnerability assessment can be any shades of gray (from ''black box'' type of testing to ''white box'') and aims to produce a report with findings the remediation of which must be prioritized based on their assigned risk-scores.

The NIST Technical Guide to Information Security Testing and Assessment [63] (Special Publication 800-115) outlines a generic security testing and assessment methodology that can be applied to almost any information system. It categorizes technical assessment techniques into 3 parts: a) review techniques b) target identification and analysis techniques and c) target vulnerability validation techniques.

c: IoMT-SPECIFIC VULNERABILITY ASSESSMENT

This assessment phase relates to identifying, quantifying and prioritizing the various vulnerabilities and/or exploits of a system. Tasks in generic security assessment methodologies do not greatly differ with each other. However, when more specific categories of systems, such as IoT devices, are involved there are guidelines for focusing on particular sets of vulnerabilities. The IoT systems are, almost always, comprised of at least one physical/hardware component for the access of which there is normally implicit trust. It can also be assumed (depending on the threat model) that a physical copy of the device will almost always be available to highly motivated adversaries, like nation states, given the virtually infinite time and resources available to them. This makes testing the physical layer particularly important. Nevertheless, an effective assessment should consider the entire IoT product ecosystem [64] and incorporate various layers. This includes the devices themselves (taking into consideration their physical-layer, their short-range communication protocols and their functionality), the control systems (either local or remote) and any other network-related services (such as cloud and web services).

In [65] a graph model along with a matrix representation is proposed for defining which criteria will be used for the disruption assessment on both actors and flows of health care devices. Other studies assess network-oriented vulnerabilities by taking into account three main parts of a system: web servers, databases, and application software. Additionally, some exploitation methods could also include direct attack, social engineering, malware and various combinations [8]. In [57] the authors present an asset-based vulnerability framework for IoMT. Once the key system assets are identified, the next step entails the identifications of the various vulnerabilities that might be exploited by a threat agent to harm a healthcare system. A multi-attacker multi-target graphical model for identifying vulnerability-based attacks and their interrelationships is presented in [66]. The proposed framework, uses CVE's to identify vulnerabilities and CVSS as a metric system. It could be used for assessing the vulnerabilities of edge devices in a given IoT network (for example, implantable medical devices). In [67] the authors use the ICS-CERT and NVD databases for deriving a data set of IoMT-related and medical software vulnerabilities across multiple medical devices. Many of the vulnerabilities identified are rated high or critical (meaning that they have a CVSS score above 7 or above 9). In [68] the authors present a goal-question security assessment framework for IoMT solutions composed of detailed and simple-to-use questions. The framework may be used to assess a wide range of a) stakeholders' requirements (e.g., patients, medical professionals, system administrators etc.); b) solutions (services, devices, platforms, etc.); and c) architectures (e.g., mobile-controlled, cloud-based, etc.). The authors provide a validation of the proposed methodology by analyzing all reported IoMT-related vulnerabilities from NIST's National Vulnerability Database (NVD)1 and CVE Details. In [69] the authors propose an instantiation of the risk assessment and testing methodology proposed by the European Telecommunications Standards Institute (ETSI) along with CWSS as a scoring system, that could be used in the healthcare context. The overall methodology is comprised of the following steps: 1) Identification of vulnerabilities (an initial analysis of the IoT environment in order to have a database of established threats) 2) Establishing the context (includes understanding the contextual, business and regulatory prerequisites and relevant security levels required) and 3) The Security assessment phase, which includes the security risk assessment and the security testing. Finally, in [70] the authors present a framework for graphically modeling and assessing attack paths of IoT devices. The graphical security model uses CVE's for vulnerability identification and CVSS as scoring system and is based on the Hierarchical Attack Representation Model (HARM) and comprises of five phases: (1) data processing, (2) security model generation, (3) security visualization, (4) security analysis, and (5) model updates. Among others, the authors provide a use case scenario in healthcare monitoring.

d: COMMON VULNERABILITIES IN IoMT

In Table 7 the most common exploitable/vulnerable features in IoMT found on the bibliography are presented, along with a taxonomy per layer and per threat category as presented in Table 6.

TABLE 7. Common exploitable/vulnerable features in IoMT.

Feature	Vulnerability Description	Layers	Threat Categories
Passwords	Passwords with low complexity are vulnerable to brute-force attacks. Passwords that are easy to find are subject to dictionary attacks. Hardcoded passwords can be easily leaked.	Application Physical	Spoofing Tampering Repudiation Elevation of Privileges
Network services	Enabled network services that are not in use or the lack of security on those services which are exposed the internet and could impact confidentiality, integrity, availability of information and exposure to unauthorized remote access attacks.	Network Physical	Tampering Repudiation Denial of Service Information Disclosure
Interfaces	Lack of security in the interfaces, especially in the part of the system located outside of the device (e.g. web, back-end API, cloud, or mobile), could lead in a security breach of the device and its related components	Application Physical	Tampering Information Disclosure Denial of Service
Authentication/Authorization	Lack of authentication/authorization mechanisms could lead to severe exposure of the system exploited	Application Physical	Spoofing Tampering Information Disclosure Elevation of Privileges
Encryption	Lacking of secure encryption mechanism or using weak encryption could lead to easy exploitation	Application Physical Hardware	Spoofing Tampering Information Disclosure Elevation of Privileges
I/O filtering	The IoMT device or web API doesn't use filtering of the input and output	Application Network	Tampering Information Disclosure
Update mechanisms	When an IoMT device is updated the firmware must be validated on the device, encryption must be enabled during transit along with anti-rollback mechanisms. Furthermore proper notifications must be implemented when security changes occur due to updates. The lack of the above mentioned measures could impact the security of the device	Physical Hardware	Tampering Information Disclosure
Use of components	Using software components that are not secured or deprecated libraries which could be compromised, using customized software components such as operating Systems (OS) or third-party software from a compromised source could be exploited and affect the security level of the system. chain	Application	Spoofing Tampering Information Disclosure Elevation of Privileges
Privacy protection	The privacy could be insufficiently protected when sensitive information are stored on the hardware or in the ecosystem(e.g. external database) that is not properly secured or doesn't have a permission policy	Application Hardware	Information Disclosure
Data transfer and Storage	Lacking of encryption or access control mechanisms on personal data in any layer of the system, even at rest, transit or processing	Network	Repudiation Information Disclosure
Device management	Lacking of security support on devices. This includes managing the assets , updating , secure decommissioning of the devices, constant search the system for abnormal behaviour. The lack of those measures could leave the system exposed to vulnerability exploitation.	Hardware	Repudiation Information Disclosure
Default settings	It is a common practice for devices and systems to be distributed with default settings that are not secure or programmed to restrict security modifications from the user	Hardware	Spoofing Tampering Elevation of Privileges
Physical protection	Lacking of physical hardening measures,which could allow adversaries to gather sensitive information which could later be used for long-ranged attack or short-ranged attack enabling them to access and control the device	Physical	Spoofing Tampering Information Disclosure

Some of these vulnerabilities are due to the human-in-the-loop factor. For example, since medical devices are expected to be available on first demand and user-friendly for older people, the manufacturers tend to employ weak authentication and authorization mechanisms, such as weak and/or hardcoded passwords. Other vulnerabilities are due to the limitations at the hardware layer. Since many types of IoMT devices are resource-constrained, the deployment of strong encryption or authorization mechanisms is not always possible. Finally, the application environment also leads to various common vulnerabilities. For example, upgrading the firmware, testing the security of the software APIs, is not a trivial task for IoMT (like implantable devices).

D. IMPACT ASSESSMENT FOR IoMT

Various methodologies have been proposed in the literature for assessing and measuring the impact of IoMT attacks. In most cases, patient harm is the most common attribute in impact assessment and control, while some papers also take into account the monetary value of the impact [73]. For example, IoMT attacks may be classified based on the consequences of a successful attack. In this case, four categories could be identified based on how severe the impact is: brand value loss, life risk, data disclosure and monetary value [49]. Similar studies classify the impact of IoMT attacks on other key criteria like a) confidentiality (non-compliance, damage to reputation, litigation and financial

TABLE 8. Comparison of impact assessment methodologies.

Literature	Impact Types	Impact scale	Recovery time	Cascading impact	Data type
[4]	E, O, LT, RP	QT	Yes	Yes	All types
[49]	E, LT,RP, RG	QL	No	No	Sensitive
[71]	LT	QL	Yes	No	All types
[72]	No	QT	No	No	All types
[73]	E	QL	No	No	Sensitive

E=Economic, O=Operational, LT=Life Threatening, RP=Reputation, RG=Regulatory,
QL = Qualitative scale used , QT = Quantitative (number) scale used.

consequences), b) integrity (wrong clinical decisions regarding the treatment of a patient due to falsified data, incorrect therapy due to device being compromised by an adversary) and c) availability (wrong clinical decisions as a consequence to limited access on critical information regarding the patient, delayed or lack of treatment due to disabled critical alerts) In [4] a three level impact scale is proposed, taking into account the connectivity depth among the IoT devices (cascade impact) and specifically the attack enabler and the targeted critical system or service. Based on various attack scenarios, the impact could be categorized as of high, medium and low importance. In [71] four major groups of impact are proposed: a) Patient safety (Imposing the impact on the health of a patient due to medical device failures such as minor/severe injury or even death), b) Service personnel or environment safety (Imposing the impact on medical personnel or the surrounding ecosystem due to failures), c) Maintenance (Measuring the average time needed for restoring or maintenance the system after a software failure) and d) Cost (Measuring the total economic cost for maintenance and the time for holding up medical operation). A four-scale impact assessment is presented in [59]. The authors identify four scales: health, economy, quality of life, and privacy. The aforementioned scales closely relate to the possible impact various attacks could have in key stakeholders of the healthcare ecosystem such as patients, practitioners, manufacturers, and more broadly states. Other studies consider the ''human factor'', putting the user on the spot and examining the role they play in the dynamics of the accidents [72]. An impact metric with values from scaled to ten is proposed. The value increases dynamically when the error impacts the safety of the ecosystem e.g medical devices, users (patients and operators).

Common criteria on Impact assessment. Based on the above literature, most methodologies for impact estimation take into account (a) *the impact types* (economical, reputational, potential life threatening, regulatory), (b) *patient harm* also defined as criticality or patient safety and (c) *recovery time* or the maintenance level needed. Other criteria which are more method-specific are also found. Some cover interesting aspects of impact assessment and offer valuable information to the comparison such as *cascading effect* meaning whether an impact scenario can trigger different adverse effects and the *data type* which defines whether those are sensitive, personal or not. Impact assessment methodologies found in the examined literature are compared based on the aforementioned criteria in Table 8.

In Fig. 3 an overview of the examined scientific literature is shown along with a categorization, depending on the phase of the risk assessment examined and the selected approach.

IV. CLASSIFICATION AND COMPARATIVE APPRAISAL OF RISK ASSESSMENT STANDARDS AND BEST PRACTICES FOR IoMT

Various standards, best practices and guidelines for IoMT security have been published by standardization bodies or other relevant organizations [12], [13], [74]–[85]. Since these documents may be related to different aspects of medical device security and to different phases of the IoMT lifecycle, it is important to provide a classification that will assist the various healthcare stakeholders to understand how these standards may assist them when implementing security controls for IoMT.

A. RELEVANT STANDARDS AND BEST PRACTICES

In this section, a brief overview of relevant standards, best practices and guidelines related to IoMT security is presented. For completeness and in order to streamline the assessment, we first outline generic risk assessment standards, then we refer to risk assessment standards for medical devices (but not in particular for IoMT devices) and finally we present in detail the IoMT specific standards. The ISO 27001 [45] is a general-purpose security management standard presenting a model for the establishment, implementation and maintenance of information security management systems (ISMS). While it assumes a risk assessment process as an underlying component, this is not its main goal. The ISO 27005 standard [86], defines a generic methodology to assess security risks. Additionally, the NIST 800-30 [42], 800-115 [63], 800-154 [43] publications offer guidance for conducting risk assessments, creating a threat model and developing mitigation strategies. In the rest of the section we will present standards and best practice guides that are more specific to IoMT domain.

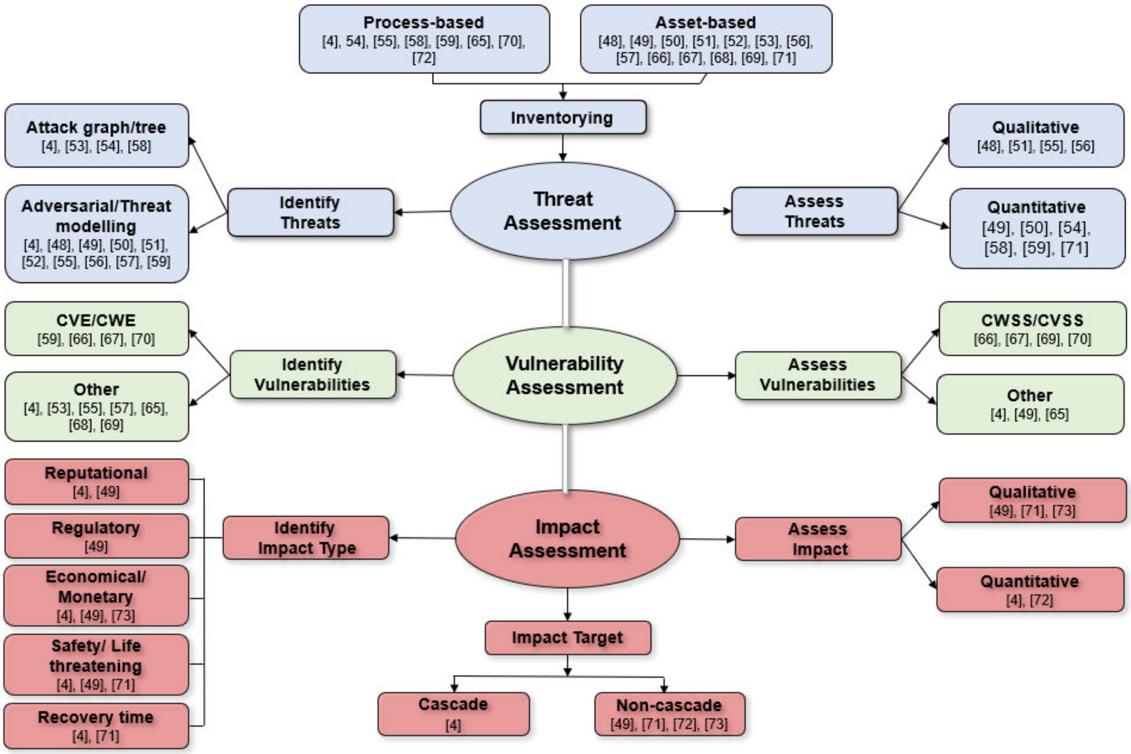


FIGURE 3. Scientific literature risk assessment methodologies classification.

e: ISO STANDARDS

The International Organization for Standardization has published the ISO14971 standard and the ISO24971 guide regarding risk methodology and risk assessment for medical devices. ISO14971 [82] is referring to manufacturers specifying the procedure for identifying risks on medical devices, including in-vitro diagnostic (IVD) in order to: (i) calculate and evaluate the associated risks, (ii) apply mitigation controls and (iii) monitor the effectiveness of the measures applied. This standard also introduces qualitative impact metrics for the medical ecosystem (named severity values), along with adverse effects that are grouped into various categories of severity. In addition, ISO-24971 [83] provides guidance in applying ISO 14971 when implementing risk management; specifically in medical devices. It is intended to help manufacturers processing these standards in risk management. It also assists, in the development of targeted policy for the criteria determination and for the risk acceptance level. Furthermore, incorporates production and post-production feedback loop into risk management, differentiating the "information for safety" and the "disclosure of residual risk", and evaluates the overall residual risk. ISO 80001 [74] is also relevant and complementary to the above, since it helps Health Delivery Organizations (HDOs) and Medical Device Manufacturers (MDMs) applying risk management for IT-networks incorporating medical devices. Complementary support for regulatory conformance is also provided indirectly through the IEC 82304-1 [77] which deals with health software. ISO 82304 applies to "the safety and security of health software products designed to operate on general computing platforms and intended to be placed on the market without dedicated hardware, and its primary focus is on the requirements for manufacturers" [77].

f: NIST

The National Institute of Standards and Technology has issued a Special Publication, SP1800-8 [85], which focuses on securing wireless infusion pumps. This publication extends the above mentioned general-purpose standards and guides. The SP-1800-8 distinguishes (a) industry analysis of risk and (b) questionnaire-based-risk assessment, that are used for a "defence-in-depth" strategy to further protect the pump, the server's components and the network. It also contains a list of common threats [Appendix A] and vulnerabilities [Appendix B] that should be thoroughly examined when assessing this type of devices. The risk assessment guidelines within rely on [87] and [88]. Additionally, the NISTIR 8228 Internal Report [84] emphasizes the differences between conventional IT devices and IoT when managing risk assessments. For example, in some IoT devices we need to take into account that some types of security risks, such as safety or device reliability, must be handled simultaneously with security and privacy; otherwise, by addressing any type independently, may result in affecting the others. NISTIR 8259 [75] builds upon NISTIR 8228 by defining a voluntary core baseline of IoT cybersecurity features for manufacturers and how to identify and implement such features. NIST publication 800-115 is an older document that provides guidance on planning and conducting technical information security tests and examinations, and so it only indirectly addresses relevant IoMT security issues and can be considered superseded by the above NIST publications. Thus, it is not analyzed in detail.

g: UL STANDARDS

The 2900-2-1 standard [89], published by UL, has been recognized by the FDA as a tool [12] for premarket reviews on the cybersecurity of medical devices. The testing methodology that is proposed within covers various layers of testing such as, malware, malformed input testing, software security and network and system penetration testing. UL 2900 reflects both premarket and postmarket regulatory (FDA) [13] thinking and there is a mapping between the various clause references [90]. The FDA medical device applicants can conform to this standard as a prerequisite to address cybersecurity as part of their US market registration. Although ISO14971 [91] focuses on life cycle requirements for medical device's software, it does so only by the aspect of safety and not security. UL 2900-2-1 is one of the few standards that call for security testing throughout the whole Software Development Life Cycle (SDLC).

h: OWASP

While not an assessment methodology, OWASP provides a checklist of vulnerabilities commonly seen in medical devices, and against which these devices should be tested [92]. Since the IoT ecosystem is typically a superset of IoMT, the OWASP IoT Testing Guide [93] (still in draft form) can be used as a supplement to the above. The OWASP Secure Medical Device Deployment Standard [81] provides a more thorough guide for applying security controls when purchasing and deploying devices in healthcare facilities. It includes high-level guidelines for purchasing controls, perimeter defenses, network security controls, device security controls, interface and central security station security, security testing and incident response.

i: MAYO CLINIC

The Clinical Information Security department at Mayo Clinic has published a comprehensive guide [79] on how to conduct vulnerability assessments on medical devices. This guide acts as a high-level list of guidelines for holistically testing the security posture of healthcare systems. In it, security testing is compartmentalized in layers: hardware/physical, network, web application, host configuration, native software and technical staff interviews and is impact-based. IoMT devices are grouped based on their overall impact on the patient safety and on the disruption of operations (e.g. implantable devices and drug infusion pumps usually get the highest risk due to the direct cause of patient harm when abused). Three criteria are used to evaluate the device impact: (a) the level of direct harm, (b) the number of patients affected and (c) the amount and type of data processed and/or stored. Six critical baseline requirements are highly weighed when calculating the final risk score of a medical device; 1. compliance with the Mayo work account standards, 2. running a supported Operating System (OS), 3. receiving routine OS patches, 4. having AntiVirus software applied and updated, 5. receiving routine 3rd-party software patches and 6. containing no default or hardcoded credentials.

While reports are not compulsory, still they offer valuable information regarding risk assessment methodologies combining best practices with real time implementation difficulties. For the scope of this paper we examine two reports published specifically for medical devices, namely the ENISA and AAMI report.

j: ENISA

In [80] which is focusing on smart hospitals and therefore IoMT, a mapping of assets, based on their criticallity and a threat model for IoMT are presented. The report identifies threat actors as insiders, malicious patients, remote attackers and others, and also describes mitigation stages based on attack scenarios.

k: AAMI

The Association for the Advancement of Medical Instrumentation (AAMI) has published a Technical Information Report (TIR), AAMI-TIR57 [76].This report is offering guidance on methodologies regarding information security risk management for medical devices. It follows the context of the Safety Risk Management requirement of ISO 14971. It also extends the risk management of IEC 80001-1 with the incorporation of the same key properties (Safety, effectiveness, Data and System security). The Annexes of the report includes useful details for the process along with examples.

l: TGA

The Australian government published a cybersecurity guide for IoMT manufacturers, including both software and devices [78]. The document provides guidance on Software as a Medical Device (SaMD) and general medical device components, in order to assist in the identification of relevant security vulnerabilities and cyber threats. It provides both pre-market and post-market information, along with lists of known vulnerabilities and current trends in the landscape.

m: MITRE

The MITRE Corporation recently published a rubric [94] to provide guidance on utilizing the Common Vulnerability Scoring System (CVSS) [95] to perform risk assessments on medical devices. In essence, it is a series of questions at various decision points that analyze the exploitability of a vulnerability. It uses the CVSS to "provide a consistent and standardized way to communicate the severity of a vulnerability between multiple parties, including the medical device manufacturer, hospitals, clinicians, patients, national cybersecurity agencies, and vulnerability researchers" [94].

B. CLASSIFICATION CRITERIA FOR THE RISK ASSESSMENT STANDARDS AND BEST PRACTICES COMPARISON

We classify the ‘‘gray literature’’ for IoMT risk assessment and management using three categories of criteria, namely: (i) their *scope* or *coverage*, (ii) their underlying *methodology* and (iii) their *acceptance* level.

1) SCOPE/COVERAGE CRITERIA

When examining the scope of each standard or guideline, we examine three criteria; the *risk assessment coverage*, the *development life-cycle coverage* and (c) the *IoMT ecosystem coverage*. The risk assessment methodologies are generally divided into two phases: the risk assessment phase and the risk management phase. In turn, risk assessment involves the processes of threat, vulnerability and impact assessment, while risk management involves the processes of risk prioritization, mitigation and effectiveness evaluations.

When examining the Development Life Cycle (DLC) of a medical device, risk assessment and management may be applied to various phases, like the pre-deployment (manufacturing) or the post-deployment (actual operation).

For the category of IoMT coverage, while some standards may cover a broader area than medical devices, such as the complete range of IoT devices, others are IoMT specific. In addition, some standards may only be concerned with a particular type of medical device, such as implantable devices.

2) RISK METHODOLOGY CRITERIA

We classify the examined documents according to the risk methodology that each document utilizes, including the *risk approach* and the *risk calculation* utilized. In general, risk assessment methodologies may follow a quantitative, a qualitative, or a semi-qualitative approach, in order to specify the type and the range of values to be used during risk assessment and how risk factors are identified and analyzed so that the values of those factors can be functionally combined to evaluate the overall risk [42]. Another criterion is related to the calculation type that may be utilized. Let $\mathcal{A}$ and $\mathcal{T}$ define an asset and a security threat respectively. According to [96], [97], the risk calculation may rely on one of the following five (5) types ($\otimes$ in all the equations defines a combination between two factors):

Class A. The risk calculation combines the likelihood of a threat, the vulnerability of an asset to a specific threat, and the impact of the threat on the asset:

$$Risk(A, T) = Likelihood(T) \otimes Vulnerability(A, T) \otimes Impact(A, T) \quad (1)$$

Class B. This type, which is in line with standards such as ISO27001, takes into consideration the security requirements $\mathcal{R}$ for a specific asset.

$$Risk(A, T, R) = Vulnerability(A, T) \otimes Impact(T, R) \quad (2)$$

Class C. This type uses the financial Annual Loss Expectancy in combination with the Average Loss for each incident against an asset:

$$Risk(A, T) = AnnLossExp(A, T) \otimes Likelihood(A, T) \otimes AvgLoss(A, T) \quad (3)$$

*Class D.*The risk calculation in this class only considers the most *critical assets* ($\mathcal{A}_{crit}$) based on their vulnerability level and the impact of unwanted events on them:

$$Risk(\mathcal{A}_{crit}, \mathcal{T}) = Vulnerability(\mathcal{A}_{crit}, \mathcal{T}) \otimes Impact(\mathcal{A}_{crit}, \mathcal{T}) \quad (4)$$

Class E. Contrary to the previous types, class E methods combine the likelihood of unwanted incidents with their potential consequences. Incidents are usually evaluated based on historical data:

$$Risk(Incident, \mathcal{A}) = Likelihood(Incident) \otimes Consequences(Incident, \mathcal{A}) \quad (5)$$

Relevant research [96], [97] indicates that these aforementioned types realize different views of risk methodologies. Class A risk equations focus solely on assets, both for single assets and asset-specific threats and also for classes of assets and more high-level approaches. Class B calculate risk as a combination of asset vulnerability and the existing security needs of an organisation and are thus suitable for organisations with clearly outlined security requirements (e.g. software products) [96]. Class C risk calculations utilize monetary terms to combine the probability of threat occurrence with the average loss of the resulting incident. Such approaches favor financial cost/benefit analyses and situations where the cost of incidents is known in advance. Class D approaches distinguish assets between critical and non-critical and are thus well-suited for analyzing critical infrastructures or operators of essential services for national and international reports. Finally Class E focuses on security incidents and attribute risk levels based on what-if scenarios and specific situations. To this end, they are usually considered as too specific for high-level risk assessment [96], [97].

3) ACCEPTANCE CRITERIA

We examine the acceptance of each standard and/or best practice based on two criteria: the *maturity* level of each document, i.e. whether it is a recognized standard, a defacto standard or if it is simply a report that can be used as a best practice; and the *adaptability* of each document to other systems, i.e., whether it can adapt to analyze devices of different complexity and/or relevance in terms of risk. This also takes into account the size and diversity of different systems.

C. STANDARDS AND BEST PRACTICES COMPARISON

We classify the relevant standards and guidelines for IoMT security assessment, based on the criteria defined above.

1) SCOPE COMPARISON

Some of the aforementioned standards, reports and guides (best practices) describe risk assessment approaches specifically for medical devices and cover all the phases of risk assessment, except of the Development Life Cycle (DLC) phase [76], [78], [79], [82]. Another group of publications cover various risk assessment and management phases but only refer to a particular DLC phase (e.g. pre-market [12], [14], [75] and post-market ([13], [74], [80], [81]). The TGA's guide [78] is an exception since it provides general guidance for both pre-market and post-market phases, yet without presenting a concise risk assessment method. This also applies to other standards related to the regulatory requirements for IoMT security, such as IEC 62304 [91], UL 2900-1 [89] and ISO 13485 [98]. UL2900-1 applies to networked devices that must be evaluated and tested for hardware and software weaknesses. ISO 13485 specifies requirements for quality management systems to demonstrate ability to provide medical devices and related services. In addition, some security standards may be related to various risk assessment phases but may target specific types of medical devices; e.g. NIST 1800 [85] that refers specifically to infusion pumps. Also, some standards do not specifically focus on medical devices but rather target the generic area of IoT risk assessment methodologies e.g. [75], [84].

Last but not least, the ISO 82304-1 [77] standard applies to the safety and security of health software products intended to be placed on the market without dedicated hardware. Mostly pre-market oriented, the standard covers the entire life-cycle requirements for manufacturers.

2) RISK METHODOLOGY COMPARISON

Most of the publications utilize qualitative or semi-qualitative scales to assess the impact and the overall risk of medical devices and/or IT systems and networks in healthcare [13], [76], [80], [83], [85]. This is to be expected, adverse effects from attacks on medical devices are more easily expressed by scenario-driven, descriptive scales, rather by quantitative numeric ones. ISO82304-1 [77] requires a preliminary risk assessment at system level, when requirements are mostly still undefined.

The most frequent risk calculation type is Class A, a combination of the likelihood of a threat, the vulnerability of an asset to the specific threat, and the impact on the asset. This is expected since IoMT-specific risk assessment methodologies target at specific types of medical assets. Nevertheless, some publications adhere to different types, such as ENISA's Class E [80], which is reasonable since this report is based on knowledge derived from specific incidents. Mayo clinic's vulnerability oriented Class B approach [79] is due to the fact that this document is vulnerability-centric and its goal is to assist in IoMT vulnerability management. Finally, FDA's post-market guidance [13] emphasizes on the criticality of the medical sector and is therefore mostly related to Class D.

3) ACCEPTANCE LEVEL COMPARISON

In terms of acceptance, publications that specifically target medical devices or instances of medical equipment are mostly guides and best practices. The ISO series [74], [82], [83] and OWASP [81] publications are standards, while some like the Mayo's approach [79], NISTIR 8228 [84] and 8259 [75] along with AAMI's [76] are mostly technical reports aimed at providing guidance for addressing risk within their respective risk frameworks. With the exception of [75], [85] and [81], most publications can adapt to analyze devices of different complexity, diversity and/or relevance in terms of risk. NISTIR 8259 is mostly intended to aid IoT device manufacturers understand cybersecurity risks so that they can provide features for maximum resilience against these risks [75]. Other publications such as IEC 62304 [91], UL 2900-1 [89] and ISO 13485 [98] do not focus on cyber-security and are cited as supplementary material able to meet various regulatory requirements of IoMT cyber-security.

Table 9 outlines and compares all documented standards and best practices that specifically target the medical IoT ecosystem. More than half of these publications (8 out of 14) focus on post-market cybersecurity requirements to address constant security threats in operating environments and continually assess risks during operation. Still, a considerable amount (6 out of 14) focuses on pre-market requirements that must be taken into consideration during the design and development process of medical devices, while only one identified publication [78] addresses both pre- and post- market cybersecurity topics in detail.

Most relevant distinctions in aforementioned literature rely in two horizontal groups of publications: those that target the manufacturer/distributor, and those that tackle with security from the end-user perspective. ISO standards provide a high-level, holistic overview of risk based on their scope; whether this applies to Risk Assessment or Risk Management. FDA publications mostly refer to regulated medical device products and are mostly references as good manufacturing practices, whereas ISO standards emphasize mostly on continuous risk management and threat mitigation in end-users. Similarly, NIST's NISTIR 8228 is a high-level baseline publication that tackles the entire medical IoT device ecosystem to support risk mitigation processes.

Besides ISO 24971 and FDA's post-market requirements, all publications delve into Risk Management topics for threat and vulnerability mitigation. The two aforementioned publications only focus on Risk Assessment procedures without delving into Risk Management. Almost half of all standards and best practices tackle both Risk Assessment and Management topics. Most (4 out of 7 publications) utilize Class A risk equation types. This is to be expected, since RAs in the IoMT focus on tangible, discrete medical assets types; an area where Class A risk equations shine on. Other approaches exist that utilize Class B (Mayo Clinic) and Class E risk equations (ENISA). ENISA's choice for Class E types follows the generic concept of their IoMT guidelines that focus on identified scenarios and have a case-driven approach. Class E risk equations are better suited to describe risk scenarios in the IoMT. Note that none of them uses the financial Annual Loss Expectancy (Class C), as in healthcare systems the

TABLE 9. Standards and best practices comparison.

Standards & Guidelines	Coverage			Risk Methodology		Acceptance Level	
	RA	SDLC	Device Type	Approach	Type	Maturity	Adaptability
ISO 14971	RM	pre-deployment	IoMT devices	n/a	n/a	Standard	Yes
ISO 24971	RA	pre-deployment	IoMT devices	QT	Class A	Standard	Yes
ISO 80001	RM	post-deployment	IoMT devices	n/a	n/a	Standard	Yes
NISTIR 8259	RM	pre-deployment	all IoT devices	n/a	n/a	Report	Yes
NIST 1800-8	RA, RM	post-deployment	Infusion Pumps	semi-QL	Class A	Guide	No
OWASP	RM	post-deployment	IoMT devices	n/a	n/a	Standard	No
FDA pre.	RM	pre-deployment	IoMT devices	n/a	n/a	Guide	Yes
FDA post.	RA	post-deployment	IoMT devices	QL	Class D	Guide	Yes
TGA guide	RA, RM	Both	IoMT devices	n/a	n/a	Guide	Yes
MAYO	RA, RM	post-deployment	IoMT	QT	Class B	Report	Yes
NISTIR 8228	RM	post-deployment	all IoT devices	n/a	n/a	Report	Yes
ENISA	RA, RM	post-deployment	IoMT devices	QL	Class E	Report	Yes
AAMI-TIR57	RA, RM	pre-deployment	IoMT devices	QL	Class A	Report	Yes
ISO 82304-1	RA, RM	pre-deployment	IoMT software	QT	Class A	Standard	Yes
MITRE Rubric	RA	Both	IoMT devices	QT	Class A	Guide	Yes

impact is mostly related to human safety and data privacy, rather than to direct monetary loss.

V. SECURITY CONTROLS FOR IoMT

Traditional IT Risk Management and relevant controls may apply to medical devices and, specifically, to the IoMT. This means that, due to their scope and type of data used, the medical devices are often considered to be of high risk (i.e. highly critical) in terms of risk assessment. Despite their criticality though, these devices rarely deploy satisfactory security controls. Most devices in the IoMT either implement basic to no security or controls, or are connected and work along legacy medical equipment that lacks proper security features.

Any effort to protect the IoMT must include knowledge and suggestions from traditional IT standards such as ISO 27001 and the NIST 800 series. For the purposes of this article, we focus on security controls that (i) are specifically designed for devices in the IoMT, or (ii) are traditional security controls that are considered critical for IoMT security. In this section we provide an analysis of the most common security controls as derived from relevant standards and best practices. In particular, we aggregate the most important security controls from numerous sources, including NIST [44], [100]–[102], OWASP [81] and ISO [45] standards, vendor instructions [79], research and best practices [1], [8], [14], [34]. Table 10 presents the most important security controls detected. The presented groups of controls are common in relevant taxonomies since prominent institutions [79], standards [14], [44] and relevant research [34] utilize similar categories. The full list of controls can be found in APPENDIXA.

Securing medical devices translates to protecting their hardware, software and underlying network connections. Some controls are taylored to IoMT's needs, while others are generic and are applied to all IT and IoT networks and devices. Concerning generic controls, network segregation and filtering are very common and are considered mandatory in traditional IT networks, ICS and IoT alike. Another important generic security measure that is of high importance in the IoMT is the use of strong encryption for all the sensitive patient data, whether at rest, in storage or in transit. For protecting medical devices against most network confidentiality attacks, good solutions include the use of a combination of TLS mutual authentication and certificate pinning, secure cryptographic algorithms and EAP-TLS for transmitting over insecure networks. The use of Bluetooth is not encouraged, even though, if necessary, it can be used under specific conditions. Also, patches and updates should be implemented as soon as possible and relevant firmware updates should be installed. In the remainder of this section we correlate some state-of-the-art security controls with known IoMT threats

TABLE 10. A list of the most important mitigation controls for IoMT security.

ACCESS CONTROL	
A.1	Device IDs and service inventory [99]
A.2	No hardcoded accounts in device [79] [81] [85] [1]
A.3	No hardcoded passwords (software or hardware-based) [99]
A.4	Remove unrestricted privileges from device owners/operators [99]
A.5	Reduce unauthorized access to devices [99]
A.6	Disable hardware ports and drives not required for use [79]
A.7	Encrypt device's storage [100]
A.8	Implement resistance to side channel attacks that require physical access (e.g. power analysis, electromagnetic etc.) [99]
COMPUTING AND NETWORK CONTROLS	
N.1	Use external devices (mediators, proxies) for delegating security functionality between users and medical equipment [34]
N.2	Firewall and NIDS/HIDS systems [81]
N.3	Dedicated DNS server and use of DNS Sinkholes for crafted IPs and scanning detection [81]
N.4	Use public key certificates and access control lists [81] [85] [34]
N.5	EAP-TLS, RADIUS Authentication and/or WPA2-Enterprise for wireless connectivity [79] [85]
N.6	Use TLS pinning [79]
N.7	Secure storage and maintenance of backup devices [45]
EXTERNAL ACCESS	
E.1	Encrypted & dedicated connections (e.g. VPN) [44] [45]
E.2	Protect physical access to sensitive devices [79] [85]
E.3	Vendors or external operators should not have access to patient data [79]
E.4	Isolate and segment networks [81] [44] [45]
SOFTWARE CONTROLS ON EQUIPMENT AND MEDIA	
S.1	No hardcoded information (e.g. serum levels) in device [79] [85]
S.2	No unnecessary services, apps and protocols [45] [85] [81]
S.3	Only strictly controlled remote firmware updates [79] [14]
S.4	De-identification (directly remove patient ID information) [14]
S.5	Encrypt data at rest and storage according to standards [79] [85]
S.6	Only process data for legitimate purposes [79] [85]
S.7	Test device software and functionality for logical errors [79] [1]
PORTABLE AND WIRELESS DEVICES	
W.1	If Bluetooth necessary, only use Security Mode 3 [101]
W.2	Disable connectivity capabilities when not in use [101] [79]
W.3	User authentication overlays (smart cards, two-factor, or public keys) [99]

and discuss their effectiveness and contribution in protecting IoMT devices, as presented in Table 11. Table 11 contains the security controls of Table 10, referenced as columns inside the table. Each control group from Table 10 is assigned as a column in Table 11, with rows effectively mapping which threats are mitigated by each column/mitigation control. Thus, there is a clear depiction of the controls that are able to counter each existing security threats.

A. SECURITY CONTROLS FOR CONFIDENTIALITY

Among threats that target medical devices, *medical information disclosure, IMD type determination, tracking of data, eavesdropping and data leakage* are the most common threats against Confidentiality. Countering such threats involves combining different approaches and securing the hardware, the software and the network layer of the medical devices. At the software and at the hardware layer, anonymization and de-identification of data when possible, especially before transmission, focus on proactively protecting information disclosure. Device vendors or operators should not have access to patient data. Strictly controlling firmware updates and using encryption internally for data at rest and in storage is commonly considered mandatory for effectively protecting patient health data. Access control measures such as prohibiting the use of hardcoded passwords and accounts on devices, physically controlling access to devices and disabling ports

TABLE 11. Mapping common security threats for IoMT to the relevant security controls identified in the literature.

	Access Controls								Network Controls							External Access				Software Controls							Wireless Controls		
Threats	A.1	A.2	A.3	A.4	A.5	A.6	A.7	A.8	N.1	N.2	N.3	N.4	N.5	N.6	N.7	E.1	E.2	E.3	E.4	S.1	S.2	S.3	S.4	S.5	S.6	S.7	W.1	W.2	W.3
Impersonation of user	✓	✓			✓							✓		✓			✓			✓								✓	✓
Impersonation of device	✓				✓						✓	✓		✓															
Patient data tampering				✓	✓		✓			✓		✓		✓		✓	✓	✓	✓	✓			✓	✓					✓
Malicious input				✓	✓				✓	✓		✓		✓		✓	✓	✓	✓		✓			✓		✓			✓
Communication modification									✓		✓	✓		✓		✓			✓								✓	✓	✓
Device failure								✓							✓		✓					✓							
Device tampering					✓	✓	✓	✓									✓				✓	✓				✓		✓	
Replay attack									✓		✓	✓		✓		✓			✓								✓	✓	✓
Log deletion				✓	✓		✓		✓			✓				✓				✓				✓					
Data delivery									✓	✓	✓	✓	✓	✓		✓			✓		✓		✓				✓		✓
Medical information disclosure		✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓		✓	✓	✓	✓	✓			✓	✓	✓				✓
IMD type determination	✓				✓	✓			✓							✓			✓	✓	✓							✓	✓
IMD tracking	✓				✓	✓			✓							✓			✓	✓	✓							✓	✓
Data Eavesdropping								✓			✓	✓	✓	✓		✓			✓				✓					✓	
Side-channel attack								✓																✓					
Battery drain				✓	✓	✓									✓						✓	✓				✓			
Signal jamming									✓		✓	✓	✓	✓		✓											✓	✓	✓
Flooding									✓			✓	✓			✓			✓								✓	✓	
Remote maintenance compromise																✓	✓	✓	✓										
Insecure API					✓				✓	✓		✓	✓						✓							✓			

and drives not required for use, all contribute to protecting the confidentiality of patient data. Implementing resistance to side channel attacks and providing tamper-proof mechanisms (such as chip destruction upon tampering of device) are considered highly effective against state-of-the-art attacks targeting device data.

At the network layer, the use of key management and encryption schemes along with standardised encryption algorithms and dedicated connections (e.g. VPN), protects against eavesdropping, man-in-the-middle and other information disclosure attacks. If the use of Bluetooth is considered necessary, devices should only use Security Mode 3, enable secure pairing and disable connectivity capabilities when not in use.

B. SECURITY CONTROLS FOR INTEGRITY

Common threats that affect the integrity of processes and data in medical devices include: *Device impersonation, patient data tampering, malicious input, modification of communication connections, device tampering, replay attacks, log deletion, remote maintenance compromise* and altering processes through *insecure APIs*.

Retaining integrity in the IoMT is commonly divided in two different categories: (i) Data Integrity and Authenticity in software and communications, and (ii) Transmission Integrity in networked devices. At the software and hardware layer, data integrity often requires the use of software integrity checks both during execution of software, and also during receipt of external input data from sensors or other devices. This includes potential provisions to ensure integrity/validation of software updates and security patches [103]. Integrity mechanisms exist that isolate processes and resources, making them invisible to entities outside trusted areas. These controls can utilize system calls or entry points for managing communication environments [37]. Also, many controls that protect against confidentiality threats also protect against integrity ones too; e.g. removing unrestricted privileges from device owners/operators and encrypting the device's storage or implementing resistance to side channel attacks like electromagnetic analysis. In terms of IoMT integrity threats, common experience indicates that strictly controlling firmware updates and testing the transmitted data are of utmost importance to protect against state-of-the-art integrity attacks. This includes testing device software and functionality for logical errors. Software component transparency [104], [105] can provide an additional control for software integrity assurance; vendors provide a Software Bill of Materials (SBOM) which identifies and lists software components, information about those components and supply chain relationships between them. At the network layer, integrity-specific controls include hashing and authentication mechanisms on data exchange (e.g. Authentication Header (AH) execution on secure IP communications), TLS pinning, dedicated DNS servers and use of external devices for delegating security functionality. These are common

TABLE 12. IoMT risk assessment: research and implementation gaps.

	Ideal State (Research Gaps)	**State of Practice (Implementation Gaps)**
Threat Assessment	-Novel threat models are required for the early identification and assessment of complex IoMT - oriented cascading attack paths (e.g. advanced malware and ransomware). - Design real-time threat identification components for IoMT-enabled systems (e.g. by employing AI/ML techniques). - Targeted adversarial models are required that consider the complex interconnections of IoMT (e.g. capture the capabilities and attack vectors of malicious insiders wrt cyber-physical interactions of IoMT with the critical medical systems).	- Budget constraints and lack of skilled personnel in hospitals leads to insufficient threat monitoring. -State of the art threat monitoring systems fail to identify advanced threats in real time, leading to less accurate threat assessment results.
Vulnerability Assessment	- Enhance vulnerability assessment methodologies to dynamically ake into account post-deployment vulnerability characteristics. - Machine learning techniques may be explored to automate the cumulative vulnerability level against connected IoMT devices.	- Lack of standardized SDLC practices for vulnerability identification and continuous assessment. - The embedded nature of IoMT does not facilitate the post-implementation of endpoint security software.
Impact Assessment	-There is a need to further examine the cascade impacts, originating from or targeting to IoMT devices. - Time related impact characteristics need to be investigated (e.g. time escalation of safety related impact).	- Although health related impact types are generally examined, there is a lack of standardized impact types and scales for IoMT.

practices against threats that try to spoof devices, their data or try to alter the device state of use by modifying transmissions.

C. SECURITY CONTROLS FOR AVAILABILITY

Most common threats against the availability of medical devices include DOS attacks, such as signal jamming, flooding and battery drainage. These attacks often target multiple layers and thus need to be mitigated by different controls. Common controls also apply here, such as encryption, the use of external proxies for traffic filtering and maintenance, dedicated DNS servers etc. Pinning also provides effective mitigation controls, since it restricts connections to specific devices and, thus, prohibits flooding by unknown sources. Authentication schemes can also be used against DoS attacks by properly restricting traffic or signals from unknown entities. Modern approaches make use of machine learning to detect and prevent DOS attacks and resource depletion [106], [107]. Table 11 provides a mapping between the common security threats against IoMT (as identified in Section III-B) and the mitigation controls proposed in the literature for IoMT security and listed in Table 10.

VI. DISCUSSION

Following the analysis provided in sections 3 and 4, in the sequence we present a detailed gap analysis relevant to the IoMT ecosystem along with future research suggestions. Some limitations of this research are also discussed.

A. GAP ANALYSIS

In this subsection we present various research and implementation gaps pertaining to relevant process requirements during threat, vulnerability and impact assessment. A comprehensive overview of the aforementioned interrelationship is depicted in Table 12, in which the various research and implementation gaps are summarized based on the examination of the most common threats, vulnerabilities, and state of the art security controls, as derived from the literature (scientific and grey).

Threat assessment: Despite relevant research approaches [16], published guidelines [12], [13] and best practices proposing security controls for specific threats [79], [92], the absence of a government enforced policy makes patients and the healthcare industry to rely on the manufacturers' self-regulating ability. Legal frameworks applicable to medical devices only mandate safety standards but not information security standards. Even laws like HIPAA [108] only cover a limited selection of problems that an IoMT-device could be faced with, such as PHI and EMR theft, but fail to address the bigger picture.

Budget constraints in hospitals and medical centers, in combination with the lack of skilled IT personnel leads to insufficient threat monitoring. On top of that, the lack of security awareness of IoMT users are practical constraints for the effective implementation of threat identification policies.

In threat assessment, the lack of accountability and ID spoofing are two of the most common threats able to affect data integrity. Other threats are also related to erroneous access control. The abuse of rights by malicious users leads to unauthorised access and corruption of information processing which, in turn leads to a variety of impact; from data theft to patient harm and monetary loss. This is why Mayo Clinic specifies this as one of the top six baseline requirements [79] when performing risk assessments of newly-purchased medical devices. Threats relating to compromised IT networks (such as malware, rogue devices, man in the middle attacks from eavesdroppers etc.) should be taken into account during threat modeling. The amount of interconnection along with the inflexibility of installing endpoint agents in IoMT systems poses a significant problem in intrusion detection, prioritization and incidence response. The operators cannot adequately identify and prioritize adverse events in their IoMT environment. The threat assessment methodologies must also consider the lack of regulation on manufacturers as a potential threat. The lack of protection software should be taken into account through threat modeling and threat assessment methodologies should include the lack of SDLCs as a potential threat.

Apart from the practical limitations on assessing IoMT related threats and besides the recent research advances, there are still inherent limitations in existing threat assessment methodologies for IoMT. Existing threat models for IoMT fail to capture and to early identify advanced and complex IoMT-oriented cascading attack paths. Examples of such attacks involve advanced malware and ransomware, e.g. malware that can alter diagnostic information in-transit [109]. As showed in [109] state-of-the-art AI could not reliably detect the malicious alterations of the DICOM files. New attack vectors for infecting DICOM files with malware [110] highlights the need for solutions that can disinfect files that might contain PHI without affecting the diagnostic data in the process. Since current AntiVirus/anti-malware products will delete the infected files in order to quarantine the infection, the implications of this type of attack are great - effectively causing a permanent Denial of Service against sensitive patient diagnostic data. The above examples are indirect threats that IoMT threat models usually miss and should be taken into account. Thus there is a need to design automated and self-learning threat identification components for IoM systems that interact with the threat assessment modules in real-time, enhanced for example with targeted machine learning and AI techniques.

Another important area of research related with threat assessment for IoMT, is the design of IoMT adversarial models that consider the complex interconnections of IoMT. For example, capturing the extended capabilities of malicious and/or compromised insiders having access to IoMT devices that may interact with critical medical systems both in cyber and physical ways. Since the physical tampering of IoMT devices can compromise the confidentiality and integrity of patient data of other interconnected systems, adversarial models for IoMT should be developed take into account malicious insiders and potential users with physical access to devices in the IoMT. Therefore, future research on threat assessment methodologies for IoMT should focus on the development of threat models that will enable the identification and assessment of hidden and/or underestimated cascading attack paths against critical medical services.

Vulnerability assessment: In practice, there is a lack of standardization for a secure Software Development Life Cycle (SDLC) for medical devices. This lack directly affects the amount and severity of potential software vulnerabilities. ISO-IEC62304 [91] focuses on safety and not security and while UL 2900-2-1 [89] proposes specific steps for testing the security throughout SDLC there is a need for standardized secure-by-design principles specifically tailored for the intricacies and limitations of IoMT devices and healthcare software. In IoMT, software vulnerabilities are directly tied to patient safety and greatly affect all the dimensions of impact assessment: life risk, data disclosure, patient and personnel safety etc.

Another practical limitation related with IoMT vulnerability assessment is that the embedded nature of most medical devices makes installing additional endpoint protection software post-deployment quite inflexible. The underlying operating system may be incompatible with most common security products and any mission-critical medical devices must go through rigorous testing before any patch is applied or extra software installed, something which would make solutions that depend on constant updates (i.e. AntiVirus, anti-malware or other endpoint agents) hard to deploy and maintain. In addition, AntiVirus solutions can create their own risks to patient safety when they give false positives and misclassify critical system files [111]. This inflexibility greatly restricts potential risk mitigation due to the lack of security measures. Possible limited work-arounds include application whitelisting [112] and file-integrity monitoring where any alterations of the system are detected and rolled-back, if deemed malicious. Still, this does not solve the operating system compatibility problem. Given the large diversity of medical systems and their components, a unified client-side solution that supports most IoMT systems out of the box is required.

Vulnerability assessment methodologies should specifically take into account software vulnerabilities introduced at the production level and might go unnoticed due to lack of SDLC. For example, when vulnerability scoring systems such as CVSS are used, an interesting research gap is to develop standardized security controls that can be directly mapped to IoMT software vulnerabilities. In this way the post-deployment vulnerability level IoMT devices can be dynamically assessed in a (semi)automated way by continuously testing the effect of standardized temporal and environmental vulnerability characteristics.

In addition, there is lack of vulnerability assessment methodologies that will enable the assessment of the cumulative vulnerability level of connected medical devices, with respect to the cascading attack paths that are enabled due to the IoMT connectivity and functionality. Machine learning techniques may be explored to automate the cumulative vulnerability level of attack paths against IoMT devices.

Impact assessment: As discussed in sections IV and III above, there is a consensus on existing IoMT impact assessment methodologies on the use of medical-specific impact types such as human safety and medical data privacy loss. However, there is a lack of standardized impact scales.

From a research perspective, although there is some active research on the effect on the study of cascade impacts for critical services, various state of the art methodologies

TABLE 13. Internal and external access controls.

Identification & Authentication	User Identifiers	Device IDs and service inventory. Old accounts to be locked/deleted. No guest accounts. No hardcoded accounts in device.
	Passwords	Sufficient password complexity. No hardcoded passwords (software or hardware-based). Frequent changes. Lockout after 6 attempts.
	Token-based identification	Two-factor authentication for critical devices.
	Device owner privileges	Remove unrestricted privileges from device owners/operators.
	Log-on	Limited false log-on attempts.
	Workstation identification	Workstation identification with centrally updated network table.
	External/Remote authentication	Location authentication. Use dedicated private connections.
Electronic access & Hardware	Theft detection	Authorise off-site use of equipment. Take measures against asset theft.
	Equipment Siting	Site devices to reduce unauthorised access
		IoMT devices must utilize unique identifiers per user.
	Physical Access	Implement resistance to tampering
		Implement resistance to side channel attacks that require physical access (e.g. power analysis, electromagnetic
		Disable hardware ports and drives not required for use [79]
		Encrypt device's storage [100]
		Token-based, network-based and domain authentication [100]
Internet	Demiltarized zone (DMZ)	Use of subneting to separate internal network from high-risk servers
Remote Access	VPN	Encrypted & dedicated connections
	Proxy servers	Relay requests from computers and act as a buffer
Devices	Internet access	Active monitoring firewall services

overlook the importance of cascading attacks, as they may not be directly associated with IoMT devices. The same holds for hidden attack paths and high probability - low impact attacks the importance of which is not always obvious and usually is underestimated, as described in [4]. Apart from the very nature of attacks, time is also another overlooked element in current impact assessment methodologies. In fact, the absence of security measures increases both the criticality or patient safety and recovery time or maintenance level needed after threat manifestation; something to consider during impact assessment. In general, current impact assessment methodologies don't take into account *time-to-recovery* aspects of the various attacks and, therefore, it's not clear what the depth and breadth of the overall impact will be. Last but not least, current impact assessment methodologies fail to capture how quickly the maximum impact occurs and they also don't take into account the possible deterioration (higher impact) accruing into the system by not acting on time (i.e. the system represents increasing value loss as an attack goes unnoticed and increasing time and effort for eventually tackling the attack).

Miscellaneous: Although several standards and best practices for IoMT security exist, there is a diversity in such standards, making it hard for the various stakeholders to comply with. Even though the strict compliance of the pre and post deployment standards could help restrain various implementations gaps, however the regulatory, operational and cost limitations are barriers to such a strict compliance. Another significant gap in the IoMT domain is the lack of a standardized way for vendors to provide remote support and maintenance to medical devices. Dissimilar processes for connecting remotely is a breeding ground for potential vulnerabilities. This is mostly an architectural issue, where existing solutions such as encrypted, dedicated VPN connections are not sufficient to prevent potential compromises from third-party networks. Threat and impact assessments classify remote connections on medical devices from malicious users as one of the top ranked threats with the highest risk, according to OWASP [113]. The increasing number of attacks through third parties [114], [115] and the continuing existence of persistent "backdoor" connections from malware threats to HDO networks for medical device manufacturers to remotely maintain healthcare systems proves this and calls for a universally secure way of on-boarding vendors. Therefore, monitoring, logging, multi-factor authentication and secure credential management all must follow industry standards and best practices.

B. LIMITATIONS

Even though the current survey is based on a systematic and structured approach, there exist some limitations worth mentioning. For example, during our search process we may not have achieved conceptual saturation as a) we have included only English-written articles in our analysis and b) the various

TABLE 14. Computing and network infrastructure controls.

Network Isolation	Architectural isolation	Internet-accessible services to be isolated from internal networks [81] [45]
	Firewall	Only allow connections relevant to business processes [79] [45]
	Delegation in external devices	Mediators for delegating security functions and access control between users and medical equipment [34]
	Syslog Server	Logs stored and exported to distinct servers
Intrusion Detection & Prevention	Detection & prevention systems	Active monitoring through IDPS and secure storage of logs [81] [44]
	DNS	Dedicated DNS server and use of DNS Sinkholes for crafted IPs and scanning detection [81]
Transportation & Transmission of Data	Physical & Digital channels	Protect confidentiality and integrity of transmitted medical data [79]
		Use public key certificates and/or access control lists (ACLs) [81] [85] [34]
	Encryption	Only encrypted data outside secure areas. No clear-text submission or storage [100]
		EAP-TLS, RADIUS Authentication and/or WPA2-Enterprise for wireless connectivity [79] [85]
	Data transmission	Use TLS pinning and controls proposed in standards (NIST SP800-52, SP800-77, SP800-66, SP800-113 and SP800-123)
Disposal of Media & Devices	Tapes, hard drives, media	Media must be zeroed or deep sector erased before disposal [45]
	Hardcopies, CDs & DVDs	Destruction before disposal according to NIST SP800-88
	Documentation	Document equipment disposal with time and date of the event

TABLE 15. Software controls.

Anti-malware	Up-to-date security software for whitelisting and periodic scans [79]
Operating system hardening	Limited administrative accounts [79]
	Apply service and security patches
	No unnecessary services, applications, and network protocols [44]
	Configure OS user authentication [44]
	No hardcoded user accounts [79]
Product upgrades	On-site service staff to install/upgrade device patches
	Only strictly controlled remote firmware updates [79]
Monitoring & Logging	Use device security logs [14] [45] [100]
	Logs protected during storage (e.g. encryption)
	Logs periodically checked for security warnings
	Backup logs from critical devices [45]
Data	Encrypted data at rest and in storage, according to standards
	Only process data for legitimate purposes [79] [85]
	De-identification (directly remove patient ID information) [14]

search strings used for identifying relevant papers/reports may not have fully captured all the available IoMT risk assessment literature. However, this is unlikely since a) our search terms were rather broad and b) we made use of the so-called snowball effect. Some reporting bias issues relevant to the thematic content analysis we have conducted along with the extraction and coding of data and the overall emerging themes identified should also be kept in mind. In general, thematic content analysis is a labor-intensive task and is always prone not only to human error but to authors' subjectivity as well. In our case we tried to overcome this limitation by applying group discussions among authors and thus reducing the possibility of misrepresentation and inaccuracy in data extraction and synthesis. Finally, another limitation of this study may relate to the appraisal of the quality of the retrieved literature. It is worth noting, however, that in the

TABLE 16. Training and Awareness controls.

Security education & Training	Organizational Controls	Verbal and written training strategy with top management commitment
		Staff awareness of security issues
		Provide security training for all staff
		Different training for different staff
		Employ general awareness techniques
		Awareness programme to cover messages to staff
		Information dissemination to all staff
		Produce security documentation
		Measure effectiveness of awareness and training programmes
	Other forms of information exchange	Staff reminders for all forms of information interchange
		Staff to be reminded of the risks when making telephone calls
		Staff to be reminded not to hold confidential conversations in public places or open offices
		Staff to be reminded not leave confidential messages on answering machines
		Instruct staff on the risks associated with using facsimile machines

eligibility phase only peer-reviewed articles were included in our analysis.

VII. CONCLUSION

In this survey paper we have provided a systematic review and appraisal of current security assessment and mitigation methodologies for IoMT systems. For streamlining our analysis we have included both scientific and grey IoMT-related literature. We have provided a taxonomy of the available IoMT risk assessment methodologies (research literature) by using a three-layer approach (threat, vulnerability and impact assessment). Based on a thorough analysis of various security standards and best industry approaches (grey literature) we have provided a comparative appraisal of current IoMT implementation practices and we have further derived various IoMT security controls. From the overall literature analysis (both scientific and grey) we have highlighted several research and implementation gaps related to the IoMT ecosystem and we have provided a roadmap of future research suggestions.

Although the IoMT security domain has attracted a lot of attention during the last years, the literature remains fragmented with increased heterogeneity in research approaches and lack of common definitions. However, we strongly believe that the IoMT security domain is an ongoing hot research topic and we expect a significant amount of related literature to be produced in the near future. We hope that this survey will provide a comprehensive understanding of this important research topic and its key aspects and help researchers to develop new or improve current IoMT risk assessment methodologies. [2], [10]

APPENDIX A SECURITY CONTROLS

A. ACCESS CONTROL

Physical and electronic access to the IoMT, both devices, their data and the underlying network, must be strictly controlled. The security controls listed below were gathered by major vendor publications [79], relevant standards [14], [45], [100] and research papers in the area [34]. The two basic categories of hardware modules are: (i) In-hospital medical devices and (ii) mobile wearables or implantables. Access control prevents unauthorized use of functionality and data in these devices [34] that can lead to various attacks such as data theft, altered processing, installation of backdoors, fault injection etc. Relevant access control security measures aim to inhibit such attacks, both in the physical and the electronic layer. External and internet access is considered untrusted. Table 13 summarizes controls from [79] and [14] for securing IoMT against threats from internal and external access.

B. COMPUTING AND NETWORK INFRASTRUCTURE CONTROLS

Again, security controls for computing and network infrastructures were gathered from multiple sources [34], vendor reports [79] and relevant standards and publications [14], [45], [81]. According to these sources, software computation and network security controls in the IoMT can be grouped into the following categories as shown Table 14.

C. SOFTWARE CONTROLS ON EQUIPMENT, SYSTEMS AND MEDIA

See Table 15.

TABLE 17. Information security policy.

Security policies & procedures	There should be an agreed Information Security Policy documented for the organisation
	The information security policy document to include organisational policy
	The policy document to cover all common aspects of IT security
	The policy document to be available to all employees
	The copy to be maintained
	Create and maintain a security policy document for each host system
	The organisational security policy is to reflect the additional security requirements that are unique to the business
	The Information Security Policy to have been approved by a senior manager
	Employees to be required to sign a statement that they understand and accept the contents of the security policy

TABLE 18. Wireless and bluetooth devices.

Wireless connection	Encryption of wireless network data transmission
	EAP-TLS or WPA2-Enterprise for wireless connectivity [79]
	Do not use the default SSID on wireless access points
	Use device-unique administrator password
Bluetooth connection	If necessary, only use Security Mode 3 [101]
	Perform pairing as infrequently as possible in a secure area
	Disable capabilities when not in use [101]
	User authentication overlays (biometrics, smart cards, two-factor or public key infrastructure)
Portable Devices & Media	Do not allow personal devices on networks [45]
	Do not store, process, download or transmit data on portable device or media [79]
	Implement a BYOD policy [45]

D. SECURITY TRAINING AND AWARENESS

Security controls for user awareness and training are extensively documented in multiple standards [45], [102] and vendor instructions [79]. Table 16 provides an aggregation of the most common controls.

E. INFORMATION SECURITY POLICY

See Table 17.

F. PORTABLE AND WIRELESS DEVICES

See Table 18.

REFERENCES

[1] FDA. *Federal Food, Drug, and Cosmetic Act (FD&C Act)*. Accessed: Oct. 2, 2019. [Online]. Available: https://www.fda.gov/regulatoryinformation/lawsenforced-by-fda/federal-food-drug-and-cosmetic-act-fdcact/default.html

[2] B. Marr. *Why the Internet Of Medical Things (IoMT) Will Start to Transform Healthcare in 2018*. Accessed: Dec. 4, 2019. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018/

[3] Allied Market Research. *Internet of Things (IoT) Healthcare Market by Component (Implantable Sensor Devices, Wearable Sensor Devices, System and Software), Application (Patient Monitoring, Clinical Operation and Workflow Optimization, Clinical Imaging, Fitness and Wellness Measurement)—Global Opportunity Analysis and Industry Forecast, 2014–2021*. Accessed: Dec. 4, 2019. [Online]. Available: https://www.alliedmarketresearch.com/iot-healthcare-market

[4] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 2018.

[5] T. Fox-Brewster. (2017). *Medical Devices Hit by Ransomware for the First Time in U.S. Hospitals (Forbes)*. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#3247d389425c

[6] D. Gayle, A. Topping, I. Sample, S. Marsh, and D. Vikram. (2017). *NHS Seeks to Recover From Global Cyber-Attack as Security Concerns Resurface (The Guardian)*. [Online]. Available: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

[7] *Anatomy of Attack: MEDJACK.2 Hospitals Under Siege*, TrapX Labs, Waltham, MA, USA, 2016.

[8] P. Williams and A. Woodward, "Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem," *Med. Devices, Evidence Res.*, vol. 8, p. 305, Jul. 2015.

[9] GMDN. *Global Medical Device Nomenclature*. Accessed: Oct. 2, 2019. [Online]. Available: https://www.gmdnagency.org

[10] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, "Security in IoMT communications: A survey," *Sensors*, vol. 20, no. 17, p. 4828, Aug. 2020.

[11] FDA. *Medical Device Classification*. Accessed: Oct. 2, 2019. [Online]. Available: https://www.fda.gov/medicaldevices/device-regulation-and-guidance/overview/classify-your-device/ucm2005371.htm

[12] FDA. *Premarket Submissions for Management of Cybersecurity in Medical Devices*. Accessed: Oct. 2, 2019. [Online]. Available: https://www.fda.gov/downloads/MedicalDevices/Device-Regulation-and-Guidance/Guidance-Documents/UCM623529.pdf

[13] *Postmarket Management of Cybersecurity in Medical Devices*. Accessed: Oct. 2, 2019. [Online]. Available: https://www.fda.gov/downloads/medical-devices/device-regulation-and-guidance/guidance-documents/ucm482022.pdf

[14] *Manufacturer Disclosure Statement for Medical Device Security*, HIMSS/NEMA Standard HN 1-2013, National Electrical Manufacturers Association, 2013.

[15] *EU Regulation 2017/745 for Medical Devices*, European Council, Brussel, Belgium, 2017.

[16] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[17] Y. Q. Zhang, W. Zhou, and A. N. Peng, "Survey of Internet of Things security," *Jisuanji Yanjiu Yu Fazhan, Comput. Res. Develop.*, vol. 54, no. 10, pp. 2130–2143, 2017.

[18] D. M. Mena, I. Papapanagiotou, and B. Yang, "Internet of Things: Survey on security," *Inf. Secur. J.*, vol. 27, no. 3, pp. 162–182, 2018.

[19] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[20] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refoufi, "A review of security in Internet of Things," *Wireless Pers. Commun.*, vol. 108, pp. 325–344, Apr. 2019.

[21] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.

[22] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of Things security: A top-down survey," *Comput. Netw.*, vol. 141, pp. 199–221, Aug. 2018.

[23] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[24] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[25] C. S. Kolli, V. V. K. Reddy, and N. V. Ramana, "Internet of Things: A survey on security threats and study on azure and AWS IoT frameworks," *J. Adv. Res. Dyn. Control Syst.*, vol. 10, no. 9, pp. 2237–2243, 2018.

[26] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[27] O. Yousuf and R. N. Mir, "A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 292–323, Jun. 2019.

[28] R. H. Aswathy and N. Malarvizhi, "Internet of Things (IoT): A survey on protocols and security risks," *Int. J. Eng. Technol.*, vol. 7, no. 1, pp. 15–20, 2018.

[29] A. A. Ibrahim and M. Kamalrudin, "Security requirements and technologies for the Internet of Things (IoT) applications: A systematic literature review," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 17, pp. 5694–5716, 2018.

[30] S. Hameed, F. I. Khan, and B. Hameed, "Understanding security requirements and challenges in Internet of Things (IoT): A review," *J. Comput. Netw. Commun.*, vol. 2019, pp. 1–14, Jan. 2019.

[31] G. Vani and A. B. Malakreddy, "A review on identification & analysis of security issues and challenges of IoT based healthcare," *Int. J. Innov. Technol. Exploring Eng.*, vol. 8, no. 4, pp. 546–549, 2019.

[32] P. Panchatcharam and S. Vivekanandan, "Internet of Things (IoT) in healthcare—Smart health and surveillance, architectures, security analysis and data transfer: A review," *Int. J. Softw. Innov.*, vol. 7, no. 2, pp. 21–40, 2019.

[33] Z. G. Prodanoff, E. L. Jones, H. Chi, S. Elfayoumy, and C. Cummings, "Survey of security challenges in NFC and RFID for E-Health applications," *Int. J. E-Health Med. Commun.*, vol. 7, no. 2, pp. 1–13, Apr. 2016.

[34] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Informat.*, vol. 55, pp. 272–289, Jun. 2015.

[35] R. Altawy and A. M. Youssef, "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices," *IEEE Access*, vol. 4, pp. 959–979, 2016.

[36] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical Internet of Things: A review," *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, Mar. 2018.

[37] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3723–3768, 4th Quart., 2019.

[38] K. Kandasamy, S. Srinivas, K. Achuthan, and V. P. Rangan, "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process," *EURASIP J. Inf. Secur.*, vol. 2020, no. 1, p. 8, Dec. 2020.

[39] D. Denyer and D. Tranfield, "Producing a systematic review," in *The Sage Handbook of Organizational Research Methods*, D. A. Buchanan and A. Bryman, Eds. Newbury Park, CA, USA: Sage, 2009, pp. 671–689.

[40] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *PLoS Med.*, vol. 6, no. 7, 2009, Art. no. e1000097.

[41] Department of Homeland Security. (2010). *Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach*. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf

[42] *Guide for Conducting Risk Assessments*, Standard NIST SP 800–30, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, 2012.

[43] *Guide to Data-Centric System Threat Modeling*, Standard NIST SP 800-154, National Institute of Standards and Technology, Mar. 2016.

[44] K. Scarfone, W. Jansen, and M. Tracy, *Guide to General Server Security*, Standard NIST SP 800–123, National Institute of Standards and Technology, 2008.

[45] *Information Technology—Security Techniques—Information Security Management Systems–Requirements*, Standard ISO 27001:2013, International Organization for Standardization, DIN Deutsches Institut Für Normung e.V., Burggrafenstrasse, Berlin, Germany, Mar. 2013.

[46] *Guide for Conducting Risk Assessment*, Standard NIST 800-30, National Institute of Standards and Technology, 2012.

[47] Department of Homeland Security. (2010). *DHS Risk Lexicon*. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf

[48] H. Almohri, L. Cheng, D. Yao, and H. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *Proc. IEEE/ACM Int. Conf. Connected Health, Appl., Syst. Eng. Technol. (CHASE)*, Jul. 2017, pp. 114–119.

[49] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of medical things: Taxonomy and risk assessment," in *Proc. IEEE 42nd Conf. Local Comput. Netw. Workshops (LCN Workshops)*, Oct. 2017, pp. 112–120.

[50] M. Cagnazzo, M. Hertlein, T. Holz, and N. Pohlmann, "Threat modeling for mobile health systems," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Apr. 2018, pp. 314–319.

[51] S. Darwish, I. Nouretdinov, and S. D. Wolthusen, "Towards composable threat assessment for medical IoT (MIoT)," *Procedia Comput. Sci.*, vol. 113, pp. 627–632, Jan. 2017.

[52] W. Leister, H. Abie, A.-K. Groven, T. Fretland, and I. Balasingham, "Threat assessment of wireless patient monitoring systems," in *Proc. 3rd Int. Conf. Inf. Commun. Technol., From Theory Appl. (ICTTA)*, Apr. 2008, no. 2, pp. 1–6.

[53] P. Luckett, J. McDonald, and W. Glisson, "Attack-graph threat modeling assessment of ambulatory medical devices," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 3648–3657.

[54] T. W. Manikas, D. Y. Feinstein, and M. A. Thornton, "Modeling medical system threats with conditional probabilities using multiple-valued logic decision diagrams," in *Proc. IEEE 42nd Int. Symp. Multiple-Valued Log.*, May 2012, pp. 244–249.

[55] J. Mnjama, G. Foster, and B. Irwin, "A privacy and security threat assessment framework for consumer health wearables," in *Proc. Inf. Secur. South Afr. (ISSA)*, Aug. 2017, pp. 66–73.

[56] S. A. Butt, J. L. Diaz-Martinez, T. Jamal, A. Ali, E. De-La-Hoz-Franco, and M. Shoaib, "IoT smart health security threats," in *Proc. 19th Int. Conf. Comput. Sci. Appl. (ICCSA)*, Jul. 2019, pp. 26–31.

[57] K. Habib and W. Leister, "Threats identification for the smart Internet of Things in eHealth and adaptive security countermeasures," in *Proc. 7th Int. Conf. New Technol., Mobility Secur. (NTMS)*, Jul. 2015, pp. 1–5.

[58] T. Hayakawa, R. Sasaki, H. Hayashi, Y. Takahashi, T. Kaneko, and T. Okubo, "Proposal and application of security/safety evaluation method for medical device system that includes IoT," in *Proc. ACM Int. Conf.*, 2018, pp. 157–164.

[59] M. Ngamboé *et al.*, "Risk assessment of cyber-attacks on telemetry-enabled cardiac implantable electronic devices (CIED)," *Int. J. Inf. Secur.*, 2020, doi: 10.1007/s10207-020-00522-7.

[60] *Managing Information Security Risk*, Standard NIST 800-39, National Institute of Standards and Technology, 2011.

[61] N. Shevchenko, T. A. Chick, P. O'Riordan, T. P. Scanlon, and C. Woody, "Threat modeling: A summary of available methods," Softw. Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep., Jul. 2018.

[62] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2019.

[63] *Technical Guide to Information Security Testing and Assessment*, Standard NIST 800-115, National Institute of Standards and Technology, 2008.

[64] Rapid7. *IoT Security Testing Methodology*. Accessed: Feb. 19, 2020. [Online]. Available: https://blog.rapid7.com/2017/05/10/iot-testing-methodology/

[65] H. Barkaoui, A. Guinet, and T. Wang, "Home health care vulnerability assessment using graph theory and matrix methods," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 4623–4629, 2017, doi: 10.1016/j.ifacol.2017.08.657.

[66] G. George and S. M. Thampi, "Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things," *Pervasive Mobile Comput.*, vol. 59, Oct. 2019, Art. no. 101068.

[67] H. Debar, R. Beuran, and Y. Tan, "A quantitative study of vulnerabilities in the Internet of medical things," in *Proc. 6th Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, 2020, pp. 164–175.

[68] F. Alsubaei, A. Abuhussein, and S. Shiva, "A framework for ranking IoMT solutions based on measuring security and privacy," in *Proc. Future Technol. Conf.*, in Advances in Intelligent Systems and Computing, vol. 880, 2019, pp. 205–224.

[69] S. N. M. García, J. L. Hernández-Ramos, and A. F. Skarmeta, "Test-based risk assessment and security certification proposal for the Internet of Things," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 641–646.

[70] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim, "A framework for automating security analysis of the Internet of Things," *J. Netw. Comput. Appl.*, vol. 83, pp. 12–27, Apr. 2017.

[71] K. Batbayar, M. Takács, and M. Kozlovszky, "Medical device software risk assessment using FMEA and fuzzy linguistic approach: Case study," in *Proc. IEEE 11th Int. Symp. Appl. Comput. Intell. Informat. (SACI)*, May 2016, pp. 197–202.

[72] M. Catelani, L. Ciani, and C. Risaliti, "Risk assessment in the use of medical devices: A proposal to evaluate the impact of the human factor," in *Proc. IEEE Int. Symp. Med. Meas. Appl. (MeMeA)*, Jun. 2014, pp. 1–6.

[73] P. Radanliev, D. De Roure, S. Cannady, R. M. Montalvo, R. Nicolescu, and M. Huth, "Economic impact of IoT cyber risk—Analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance," in *Proc. IET Conf. Publications*, 2018, p. 9.

[74] *Application of Risk Management for it-Networks Incorporating Medical Devices—Part 1: Roles, Responsibilities and Activities*, Standard IEC 80001-1, International Electrotechnical Commission, Geneva, Switzerland, 2010.

[75] M. Fagan, K. Megas, K. Scarfone, and M. Smith, "Core cybersecurity feature baseline for securable IoT devices, a starting point for IoT device manufacturers," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 8259, 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8259-draft.pdf

[76] *Principles for Medical Device Security—Risk Management*, Standard TIR 57:2016, Association for the Advancement of Medical Instrumentation, 2016. [Online]. Available: http://my.aami.org/aamiresources/previewfiles/TIR57_1607_Preview.pdf

[77] *Health Software—Part 1: General Requirements for Product Safety*, Standard ISO/IEC 82304-1:2016, International Organization for Standardization, DIN Deutsches Institut Für Normung e.V., Burggrafenstrasse, Berlin, Germany, Mar. 2016.

[78] Medical Devices Branch, Therapeutic Goods Administration (TGA), Australian Government Department of Health. (Jul. 2019). *Medical Device Cyber-Security Guidance for Industry*. [Online]. Available: https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf

[79] Mayo Clinic. *Medical Device Vendor Instructions*. Accessed: Dec. 5, 2019. [Online]. Available: https://www.mayoclinic.org/documents/medical-device-vendor-instructions/doc-20389647

[80] E. J. Mayol, A. Z. Manzoni, F. Calcavecchia, Y. Iliev, B. Kabisch, C. Lovis, M. Morgenstern, R. Gomes, G. Gerald, D. Glynos, S. Antonatos, G. Fletcher, and P. Jespersen, "Smart hospitals security and resilience for smart health service and infrastructures November 2016 smart hospitals about ENISA," Eur. Union Agency Netw. Inf. Secur. (ENISA), Athens, Greece, Tech. Rep., Dec. 2016.

[81] OWASP. *Secure Medical Device Deployment Standard*. Accessed: Dec. 5, 2019. [Online]. Available: https://www.owasp.org/index.php/OWASP-SecureMedicalDeviceDeploymentStandard

[82] *Medical Devices—Application of Risk Management to Medical Devices*, Standard ISO/FDIS 14971, International Organization for Standardization, Geneva, Switzerland, 2019. [Online]. Available: https://www.iso.org/standard/72704.html

[83] *Medical Devices—Guidance on the Application of ISO 14971*, Standard ISO/FDIS 24971, 2020. [Online]. Available: https://www.iso.org/standard/59587.html

[84] K. R. Boeckl, M. Fagan, W. J. Fisher, N. B. Lefkovitz, K. N. Megas, E. M. Nadeau, B. M. Piccarreta, D. G. O'Rourke, and K. A. Scarfone, "Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 8228, 2018.

[85] G. O'Brien, S. Edwards, K. Littlefield, N. McNab, S. Wang, and K. Zheng, *Securing Wireless Infusion Pumps*, Standard NIST SP 1800-8, National Institute of Standards and Technology, 2018.

[86] *Information Technology—Security Techniques—Information Security Risk Management*, Standard ISO/IEC 27005, 2008. [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=56742

[87] G. Stoneburner, A. Y. Goguen, and A. Feringa, *Risk Management Guide for Information Technology Systems*, Standard SP 800-30, 2002.

[88] *Guide for Applying the Risk Management Framework to Federal Information Systems*, Standard NIST SP 800-37, Joint Task Force Transformation Initiative, 2010.

[89] *Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements*, UL Standard UL 2900-1, 2017. [Online]. Available: https://standardscatalog.ul.com/standards/en/standard_2900-1_1

[90] J. Heyl. *Overview of UL 2900*. Accessed: Jan. 18, 2020. [Online]. Available: https://cybersecuritysummit.org/wp-content/uploads/2017/10/4.00-Justin-Heyl.pdf

[91] *Medical Device Software—Software Life Cycle Processes*, Standard IEC 62304:2006, International Organization for Standardization, Geneva, Switzerland, 2006. [Online]. Available: https://www.iso.org/standard/38421.html

[92] OWASP. *Secure Medical Device Testing*. Accessed: Dec. 5, 2019. [Online]. Available: https://www.owasp.org/index.php/OWASP-Internet-of-Things-Project/Medical-Devices

[93] *IoT Testing Guide*. Accessed: Dec. 5, 2019. [Online]. Available: https://www.owasp.org/index.php/IoT-Testing-Guides

[94] M. P. Chase and S. M. C. Coley, "Rubric for applying CVSS to medical devices," MITRE Corp., McLean, VA, USA, Tech. Rep., Jan. 2019. [Online]. Available: https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

[95] S. M. Radack. (Oct. 2007). *The Common Vulnerability Scoring System (CVSS)*. [Online]. Available: https://www.nist.gov/publications/common-vulnerability-scoring-system-cvss

[96] E. Zambon, S. Etalle, R. J. Wieringa, and P. Hartel, "Model-based qualitative risk assessment for availability of it infrastructures," *Softw. Syst. Model.*, vol. 10, no. 4, pp. 553–580, 2011.

[97] D. Gritzalis, G. Iseppi, A. Mylonas, and V. Stavrou, "Exiting the risk assessment maze: A meta-survey," *ACM Comput. Surv.*, vol. 51, no. 1, p. 11, 2018.

[98] *Medical Devices—Quality Management Systems—Requirements for Regulatory Purposes*, Standard ISO 13485:2016, International Organization for Standardization, DIN Deutsches Institut Für Normung e.V., Burggrafenstrasse, Berlin, Germany, Mar. 2016.

[99] NIST. *Security and Privacy Controls for Federal Information Systems and Organizations*. [Online]. Available: https://nvd.nist.gov/800-53/Rev4/family/

[100] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, Standard NIST SP 800-124, 2013.

[101] J. Padgette, J. Bahr, M. Batra, M. Holtmann, R. Smithbey, L. Chen, and K. Scarfone, "Guide to Bluetooth security," NIST, Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-121, May 2017.

[102] M. Wilson and J. Hash, *Building an Information Technology Security Awareness and Training Program*, Standard NIST SP 800-50, 2003, pp. 1–39.

[103] *Guidance on Cybersecurity for Medical Devices*, document MDCG 2019-16, Medical Device Coordination Group. [Online]. Available: https://ec.europa.eu/docsroom/documents/38941/attachments/1/translati-ons/en/renditions/native

[104] National Telecommunications and Information Administration. *NTIA Software Component Transparency*. Accessed: Feb. 22, 2020. [Online]. Available: https://www.ntia.doc.gov/SoftwareTransparency

[105] *NTIA Software Component Transparency—Healthcare Proof of Concept Report*. Accessed: Feb. 22, 2020. [Online]. Available: https://www.ntia.doc.gov/files/ntia/publications/ntiahealthcarepocreportfinal-draft20190904.pdf

[106] S. Gao and G. Thamilarasu, ''Machine-learning classifiers for security in connected medical devices,'' in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–5.

[107] S. Vhaduri and C. Poellabauer, ''Wearable device user authentication using physiological and behavioral metrics,'' in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–6.

[108] U. S. Department of Health & Human Services. *Health Insurance Portability and Accountability Act (HIPAA)*. Accessed: Mar. 4, 2020. [Online]. Available: https://www.hhs.gov/hipaa/index.html

[109] Y. Mirsky, T. Mahler, I. Shelef, and Y. Elovici, ''CT-GAN: Malicious tampering of 3D medical imagery using deep learning,'' *CoRR*, vol. abs/1901.03597, pp. 1–19, Jan. 2019.

[110] M. P. Ortiz. *Attacking Digital Imaging and Communication in Medicine (DICOM) File Format Standard*. Accessed: May 14, 2020. [Online]. Available: https://github.com/d00rt/pedicom/blob/master/doc/AttackingDigitalImagingandCommunicationinMedicine(DICOM)fileformatstandardMarkel_Picado_Ortiz_(d00rt).pdf

[111] K. Fu and J. Blum, ''Controlling for cybersecurity risks of medical device software,'' *Commun. ACM*, vol. 56, no. 10, pp. 35–37, Oct. 2013.

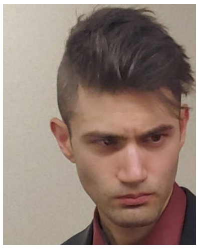
[112] R. N. Chakravartula and V. N. Lakshmi, ''Combating malware with whitelisting in IoT-based medical devices,'' *Int. J. Comput. Appl.*, vol. 167, no. 8, pp. 33–37, Jun. 2017.

[113] OWASP. *OWASP Top 10—IoT*. Accessed: Dec. 5, 2019. [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

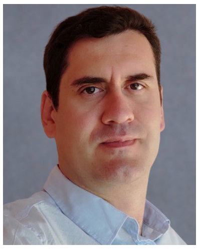
[114] *Trustwave*. Accessed: Mar. 4, 2020. [Online]. Available: https://www.trustwave.com/Company/Newsroom/News/-/Trustwave-Reveals-Increase-in-Cyber-Attacks-Targeting-Retailers,-Mobile-Devices-and-E-Commerce/

[115] Securelink. *Compromised Vendor Credentials Allow Hancock Hospital Breach*. Accessed: Mar. 4, 2020. [Online]. Available: https://www.securelink.com/blog/compromised-vendor-credentials-allow-hancock-hospital-breach/

VANGELIS MALAMAS (Graduate Student Member, IEEE) received the degree in mathematics from the University of Patras, in 2008, and the M.Sc. degree in computer science from the University of Piraeus, in 2017, where he is currently pursuing the Ph.D. degree in distributed security and trust management technologies on IoT with the Department of Informatics. He is a member of the Security Research Laboratory (SecLab). His research interests include blockchain, the IoT and IoMT security, and cryptography.



FOTIS CHANTZIS received the M.E. degree in computer engineering and informatics from the University of Patras, in 2012. He is currently pursuing the Ph.D. degree in security of IoT and medical systems with the Department of Informatics, University of Piraeus. He has worked as a Principal Information Security Engineer with Mayo Clinic, where he was conducting manual security assessment against medical devices and clinical systems. He is also the lead author of the No Starch Press book *Practical IoT Hacking*. His research interests include the IoT security, network protocols, cloud security, and the intersection of machine learning with information security.



THOMAS K. DASAKLIS graduated from the Department of Industrial Management and Technology, University of Piraeus. He received the M.Sc. degree in supply chain management and the Ph.D. degree in emergency supply chain management and disaster response. He has worked with the private sector for three years as a Supply Chain Director. He has also worked for the European Commission (DG Humanitarian Aid and Civil Protection) and the University of Piraeus Research Centre. He is currently an Adjunct Academic Staff with the Hellenic Open University, and also a Seasonal Lecturer with the Department of Informatics, University of Piraeus. He has participated in National and European Research projects. He has published articles in several international journals and conference proceedings. His research interests include supply chain management, operational research, humanitarian logistics/disaster response, data analysis, and blockchain technology.

GEORGE STERGIOPOULOS (Member, IEEE) received the B.Sc. degree in informatics from the University of Piraeus, Greece, and the M.Sc. degree in information systems and the Ph.D. degree in critical infrastructure protection at software and information interdependency levels from the Athens University of Economics and Business, Greece. He is currently an Assistant Professor with the Department of Information and Communication Systems Engineering, University of the Aegean, Greece. He was a Principal Investigator in multiple funded research projects in the areas of critical infrastructure protection, computer security, and network security. He has published over 30 articles in peer-reviewed journals and international conferences. He is an expert in ISO 27001 and EU GDPR consulting.

PANAYIOTIS KOTZANIKOLAOU (Member, IEEE) received the degree in computer science and the Ph.D. degree in ICT security from the University of Piraeus, Greece, in 1998 and 2003, respectively. He is currently an Associate Professor of Network Security and Privacy with the Department of Informatics, University of Piraeus, and the Director of the Security Research Laboratory (SecLab). He has participated in various national, European, and international research and development projects. He has published more than 70 papers in books, peer-reviewed journals, and conferences. His research interests include network security, communication privacy, applied cryptography, and critical infrastructure protection. He has served as a Guest Editor, a Program Committee Member, and a reviewer for various international journals and conferences.

CHRISTOS DOULIGERIS (Senior Member, IEEE) was an Associate Member of the Hellenic Authority for Information and Communication Assurance and Privacy, and the President and a CEO of the Hellenic Electronic Governance for Social Security SA. He was also held positions with the Department of Electrical and Computer Engineering, University of Miami. He is currently a Professor with the Department of Informatics, University of Piraeus, Greece. He has participated in many research and development projects. He has been involved extensively in curriculum development both in USA and Greece. He has published extensively in the networking scientific literature. He is a co-editor of a book on *Network Security* (IEEE Press/John Wiley).