Mobile Networks and Applications
https://doi.org/10.1007/s11036-022-02042-1

A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach

Sondes Ksibi[1] · **Faouzi Jaidi**[1,2] · **Adel Bouhoula**[3]

Accepted: 11 July 2022

Abstract
Internet of Things (IoT) applications are among the major trends of nowadays. Billions of connected devices are creating great business profits and performing a multitude of automated tasks in many daily human activities. In healthcare service delivery, IoT capabilities are difficult to overestimate, they are progressively becoming entangled and commonly coined Internet of Medical Things (IoMT). The participating nodes in IoMT networks generate, collect and exchange huge amounts of extremely private and sensitive data. Numerous security vulnerabilities arise due to the complexity and the heterogeneity of the technology. New risks, born out of IoMT systems, cannot easily be supported by existing risk management frameworks. The existing cyber-security risk assessment methods and approaches, deployed in several organizations, will not address the IoMT inherent risks properly. This study includes a comprehensive review of IoMT systems. Popular risk assessment methods are discussed and their suitability to IoMT is dealt with in detail. Based on this study, we propose a framework to enhance trust and help with decision making in e-healthcare environments given its high-risk exposure. The proposal is based on a quantified risk assessment approach. Our aim is to define a novel approach/model for improving trust and risk management in an e-health context.

Keywords e-Health · IoT · IoMT · Security · Risk management · Trust

1 Introduction

The number of connected persons and physical objects to Internet keeps increasing boosted by advancements in Information and Communication Technologies (ICT). In numerous fields of life, connected devices are performing tasks that humans aren't able to do. The Internet of Things (IoT) programming enables physical objects to communicate together, to share information and to make decisions taking advantage of their computational capabilities. Things are becoming smart. Smart objects build high distributed networks by exploiting ubiquitous and pervasive computing, Internet applications and protocols, low range communication protocols, and embedded systems.

Advancements in ICT act as a pillar for adopting IoT in numerous fields of our lives. Healthcare is one of the domains in which IoT can play a remarkable role and transform the way services are provided. Networking of smart electronic devices for wellbeing and health active assessment attracted patients, health professionals and industrials. In fact, via connected sensing devices, embedded to a human body or fixed somewhere around it, we can perform long-term supervising of physiological (e.g. heart beat), psychological (e.g. temper), environmental (e.g. noise) indicators. From this perspective, highly distributed networks based on the Internet of Medical Things (IoMT) are emerging and exchanging huge amounts of data.

✉ Sondes Ksibi
sondes.ksibi@supcom.tn

Faouzi Jaidi
faouzi.jaidi@gmail.com

Adel Bouhoula
a.bouhoula@agu.edu.bh

[1] Higher School of Communication of Tunis, LR18TIC01 Digital Security Research Lab, University of Carthage, Tunis, Tunisia

[2] National School of Engineers of Carthage, University of Carthage, Tunis, Tunisia

[3] Department of Next-Generation Computing, College of Graduate Studies, Arabian Gulf University, Manama, Kingdom of Bahrain

Published online: 29 September 2022

Although the significant technology adoption, many IoT users still feel unconfident and security remains a primary barrier when it comes to e-health trustworthiness. Exchanged data is highly sensitive and related to user private life. End user devices are basically low-cost and resource constrained while, at the same time, they are supposed to communicate over open infrastructures such as Internet and cloud servers. Unlike traditionally connected computer networks, this paradigm brings new risks. The impact of data loss can vary from service unavailability to life lost. Hence, risk assessment methods need to be readapted to the context of e-health systems for more efficiency.

The large scale deployment of e-healthcare depends on its trustworthiness and the patients confidence in the security of their communications and the protection of their sensitive data. With regards to the businesses involved, the growth of electronic connected devices for healthcare economy depends on keeping transactions costs low while still providing effective and efficient transfers of data with acceptable risks. Effective security measures involve additional process costs. Risk is an indirect cost supported by e-health systems builders.

The current paper aims to provide a comprehensive study of e-health systems and their associated concepts: architecture, applications, advancement and basic challenges. Data protection and cyber-security aspects are dealt with in detail. The performed widespread synthesis and deep analysis allow better understanding of the requirements of this emerging paradigm and mainly help us in setting up a new solution to address the security risks within e-healthcare service delivery. As a main contribution, we define a framework to enhance trust and help with making decisions based on a quantified risk assessment approach. Our proposal consists of a novel approach for improving trust and security risk management in an e-health context.

In the reminder of the manuscript, we introduce e-health systems in terms of applications and challenges. We particularly discuss security challenges in such a high-risk exposure environment. Given the various new vulnerabilities in the IoT based healthcare service delivery and the multiple contexts in which an IoMT network can be set up, we deeply analyze the existing risk management frameworks that had been extended to address the IoMT context. Later, as a part of our research, based on the literature study and analysis, a fine grained approach to manage the cyber risk for IoMT systems was designed. The approach takes into consideration the IoMT specific context and risk factors. We worked on transforming these factors as computable inputs to evaluate the overall risk rates of e-health applications. In the last section of this research, risk assessment formulas are presented and discussed. Finally, we conclude the paper and present our ongoing works.

2 IoT market opportunity

IoT holds great opportunity in the healthcare domain for device manufacturers, Internet service providers, healthcare givers and application developers. As per statistics and according to [1], there were 26.66 billion active IoT devices in 2019 and 31 billion devices projected to be installed during 2020 (40% of them for health purposes). A Mckinsey report [2] predicts this number to reach 50 billion by 2025.

IoT-based services have also a considerable economic impact for businesses. It is estimated that healthcare applications will gain the largest IoT market share by 2025, as illustrated in Fig. 1. In fact the IoT healthcare market size is expected to grow from 55.5 billion USD in 2019 to 188 billion USD by 2024 [3]. Indeed, the number of patients using connected medical devices at home is projected to grow by 44.4% each year. It is also expected that IoT will have a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025 [4].

3 Review of e-health systems

3.1 Presentation

Healthcare represents the set of services delivered to a person (patient) in order to improve his physical, mental and emotional well-being. These services are typically delivered through hospitals according to various procedures.

The concept of e-health (Electronic Health) is quite broad. It is defined according to the World Health Organization (WHO) as "*the cost-effective and secure use of ICT*

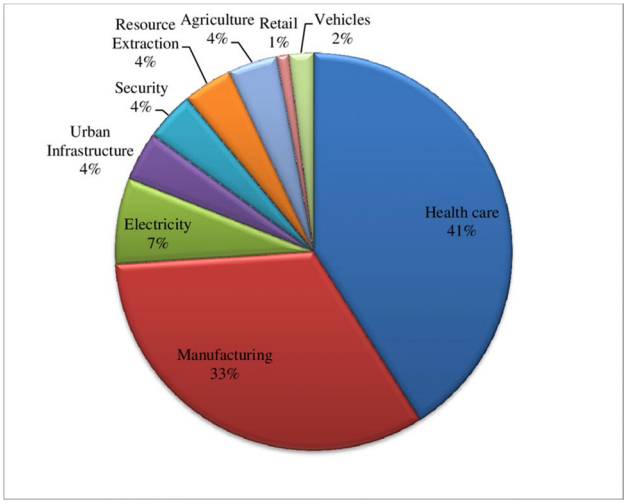

Fig. 1 Projected market share of dominant IoT applications by 2025 [5]

in support of the health and health-related fields including healthcare, health surveillance and health education, knowledge and research" [6]. It is also defined according to the European Commission (EC) as "*the use of modern ICT to meet needs of citizens, patients, healthcare professionals, healthcare providers, as well as policy makers*" [7]. In terms of advantages, the main benefits of using e-health systems are: (i) it contributes to the enhancement of health (via sustaining a healthy lifestyle); (ii) it helps in reducing costs of healthcare services; (iii) it sustains healthcare services based on communication technologies; and (iv) it improves the quality of access to digital e-health data.

The IoT finds a wide range of applications in this field such as: elder care (nursing at home or in hospitals for elderly and tracking their well-being), real time location and monitoring, data gathering for early diagnosis, etc. Also, wearable devices and medical mobile applications are typical use cases that widen areas in which IoT is playing an important role. Moreover, remote monitoring and real time communications provide more efficient treatment administration.

3.2 Advancements and applications

The main fields of applications for e-health are: digital medical records, telemedicine, telecare services, and healthcare networks and workflows. Now, smart healthcare services improve the quality of experience of patients. They manipulate data related to their vital signs and they are able to analyze information in order to decide what to do next. End users are more and more involved in the healthcare system. From practitioner's point of view, decisions are more tied because of the decision support software and the possibility of real time data sharing.

Nowadays, smart connected objects are among the most important trends of the moment. In healthcare, IoT has various application aspects and the IoMT has emerged as a main advancement. E-health applications are expected to flourish at home and remote patient monitoring is gaining more attention. They are moving from hospitals to patients living environment. We present in the following a summary of main e-health applications:

Clinical care It consists of the real time tracking of physiological status for hospitalized patients requiring close attention. IoT devices gather continuously vital signs of patients and send them to the doctors. Linked devices provide a continuous automated flow of information. Thus, IoT enables real-time alerting, tracking, monitoring, and treatment.

Remote monitoring Sometimes it is impossible for some people to contact a doctor who is many kilometers away, but with a linked device they can share their ailment-related data with medical staff. Appropriate health recommendations can be provided at time after analyzing the collected signs.

Prevention health/early intervention A sportsman or any active person can benefit from IoT devices to monitor his daily activities and well-being [8]. An elderly can also monitor his blood pressure, heart beats, etc. and in case of abnormal activity devices can sign/send an alarm to a family member, his doctor, the emergency or even a designated person/system.

Diverse A lot of other applications that take benefit from smart connected sensors and devices have been defined such as remote nursing, assisted living and childcare, remote complex surgical interventions, etc.

3.3 E-health challenges

E-healthcare promises to provide efficient and cost-effective services to underserviced patients; however it comes with a set of challenges which, if not met, could unsettle its success. We present, in Fig. 2, a summary of the main general challenges for e-health systems and we discuss below the details.

1. *Technical Reliability:* it is related to the device safety and its ability to collect and communicate data accurately without interruptions or malfunctions. Since patients will make use of the device, it is predicted that technical control/insurance will be provided by vendors or healthcare providers.
2. *Obsolete/No Existing Infrastructure*: many hospitals are still using papers and have obsolete digital infrastructure. Setting up an e-health system will be costly and needs new processes for work.
3. *Scalability*: the real time communication and the huge number of devices, simultaneously connected, will generate immense amounts of data. High storage capacities and computation resources will be required.

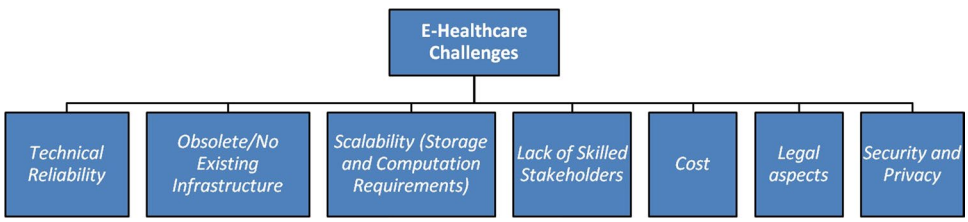

Fig. 2 Main general challenges for e-health

4. *Lack of Skilled Stakeholders*: the lack of skilled users is a serious challenge for setting up a successful e-health system. Users of the e-health system are health practitioners, patients, maintainers, and developers. They may have lack of ICT skills or low level of education especially in developing countries [9].
5. *Cost*: in spite of being trending all over, implementing smart hospitals and enabling IoT devices talking have a considerable cost.
6. *Legal aspects:* definitely, one of the most important factors related to the allocation and development of e-health is the provision of legal aspects and balancing whole collection of laws and regulations, with respect to this phenomenon. Some of the legal challenges of electronic health system in most countries are: lack of following government's ratified laws, no support of national and universal standards, lack of existing suitable laws regarding personal rights and keeping patients' private surroundings, the need for developing a legal and lawful framework for managing it in health care; the need for developing a framework for transmitting inhomogeneous data and unifying them, etc.
7. *Security and Privacy*: ensuring security and privacy of data and patients is a very crucial aspect in e-health given that security threats may have a huge impact on the privacy, health or even life of patients. Indeed, private and confidential data is at the heart of e-health systems and ought to be treated with a high level of surety. More, even IoT and IoMT bring numerous benefits to the industry; they also create numerous vulnerable security spots.

4 Security advancements in e-health

4.1 E-health security requirements

Security gains more and more importance with the emergence of IoMT. The manipulation of huge amounts of data with respect to their ownership and secrecy preservation has become a major area of concern. IoT-based e-health applications have to ensure a number of security functions such as data integrity, confidentiality, privacy, authentication, authorization, availability and non-repudiation as well as standard communication scenarios [10].

1. *Privacy*: in open and untrustworthy environments, privacy is of ultimate importance since a disclosure of medical patient's data may damage his life. Secrecy of data must be highly preserved. In e-health environments, privacy integrates anonymity. Patients must not be identifiable by any inappropriate user such as insurance providers, researchers, management staff, etc., however physicians, nurses, cashiers can view some information in order to perform treatment and billing.
2. *Confidentiality*: this feature is to guarantee that the only entities that can access to data are only authorized ones. Many users can need access to the data in e-health systems; authorizations must be well allocated to protect patient private data.
3. *Integrity*: it consists in maintaining data unaltered during end-to-end transmission process between devices. Thus integrity safeguards that any data received in transit has not been changed [11].
4. *Authentication*: it ensures that devices, sensors, applications and systems are mutually recognized when they want to communicate.
5. *Availability*: it consists of ensuring services availability even under denial of service attacks. Within an e-health context, in emergency cases, the availability of main services is crucial.
6. *Non-Repudiation*: in order to pass up incidents linked to user's irresponsibility and negligence, it is recommended that the access control system integrates non-repudiation mechanisms such as auditability. This helps mainly in auditing illegal access and collusion attempts that allows strengthening the system with the corresponding prevention rules and controls.

4.2 E-health security and cyber-security challenges

A 2019 analysis of IoT cyber-security jobs adverts [12] showed that the demand for IoT security experts increased by 49% between Q3/Q4 2018. This was coupled with a severe shortfall of available applicants, with contractors being relied upon and a fast-rising cost to access this expertise.

Security and privacy are very challenging for e-health given the sensitivity of data. Many researchers have shown that security shortcomings in IoMT affect systemically patient's health and safety [13–15]. As stated in [16], there is a lack of governance mechanisms, standards, regulations and laws, as well as industry best practices which has led to great difficulties in security requirements implementation. In the following, we discuss the main security challenges for e-health systems.

1. *Privacy assurance and data protection*: Internet was not initially designed for IoT applications with a private data exchange. In e-health applications, various communication techniques can be utilized i.e. Bluetooth, NFC, Zigbee leading in a multiprotocol environment. The minor breach from one of these wireless connections can ruin the patient [17]. IoMT devices are resource-constrained, designed to accomplish a set of functional features regardless security features, so, every device

presents a potential risk for the privacy of the patient and even his safety [18].

2. *Identity management and authentication*: many IoMT devices do not support authentication mechanisms. Whence possible, authentication mechanisms are done for devices only to establish the communication procedure, but in terms of anonymity it is still an open research issue. More, some devices accept automatic software updates without encryption or authentication, so, this update mechanism could be easily compromised.
3. *End-to-end security solutions*: the concept of smart homes involves the use of IoT devices for e-health applications as well as other smart applications such as alarm control. This emerging concept generates new risks and additional attack origins [19]. It is commonly agreed that end-to-end security solutions are difficult to fulfill but they are a crucial requirement for IoMT environments.
4. *Trust Management*: in an IoMT environment, making safe interactions is necessary. The trustworthiness of the system users, devices and /or communication protocols must be evaluated. Trustworthiness has an important role in e-health growth.
5. *Cloud challenges*: cloud infrastructure is promising for healthcare industry since it offers many benefits such as flexibility, cost and energy saving, resources sharing and fast deployment [20]. However the centralization of data on the cloud raises many security problems. Best effort Internet connections to the cloud can affect user experience. Shared environment is prone to problems of data loss and privacy violation. Absence of regulations and governance to globalize the use of cloud for e-health as well as a limited control on data because of the cloud generic applications constitute additional challenges.

Figure 3, synthesizes the basic security challenges in a highly constrained e-health environment with regards to IoMT applications specificities and constraints from one hand and security requirements and features from another hand.

4.3 E-health risk landscape

E-health applications run on an interactive network of actuators, sensors and medical devices. E-health systems are increasingly becoming vulnerable to cyber-security incidents due to diverse reasons such as: nature of generated data, volume of exchanged information, patients identity management, diversity of protocols used by the communicating nodes, resource constraints of the devices, etc. Indeed, healthcare information systems are various in nature (obsolete sometimes) when enabled to access to the Internet (although not designed for this) they become easy targets to cyber attacks. Moreover, many outdated information systems and applications did not support security functionalities, so, whence connected to open environments, they will be exposed to several security vulnerabilities and breaches.

E-health networks are expected to connect billions of heterogeneous objects all over the world through the Internet. Consequently, the ability to organize different components/to operate in a coherent way and deliver applications of interest is of the most disruptive changes. The overall security level of e-health systems is upper-limited by the security features of the weakest component. The attack surface concerns basically medical devices, communication channels and data. To go in-depth in this study, we consider a basic 3 layers model of an e-health system composed of application layer, network layer and perception layer. We note that some existing systems extend the basic model to 4 layers or 5 layers.

4.3.1 Perception layer

The physical layer (perception layer) is composed of objects or devices in charge of collecting and processing data. Big

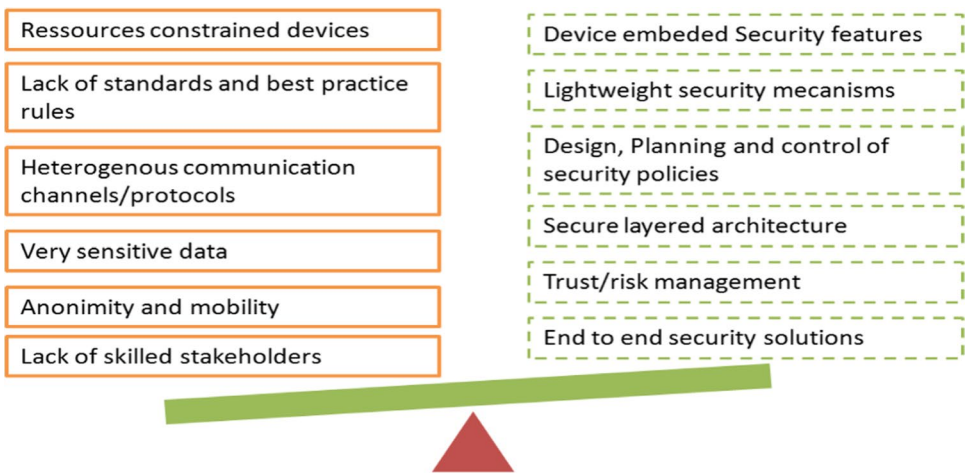

Fig. 3 Security challenges in e-health environments

data generation is initiated in this layer. Sensors and actuators transform collected/generated data to digital signals and transfer them to the network layer.

There is a panoply of IoT devices which can be classified based on how they are connected to the patient and on the need basis. Sensors are incorporated in human body or installed around it. They can be classified to embedded or not-embedded sensing devices. Wearable (as not-embedded) sensors can be divided into two types: on body contact sensors or peripheral non-contact sensors [21]. Sensors are tiny sized, low battery powered, having low speed processors and limited memory size. The devices do not create/collect data in the same way. For example, a long term tracking of well-being signs may only require sending data to a processing unit every day, so, a delay of few minutes can be tolerated. In the worst case, the total loss of measurements for a small period of time compared with the total collection period would be of no or little consequences. In contrary, for a device that monitors a life threatening condition, which requires no delayed actions to be taken, the loss of a single packet of data can be life loosing. Devices can be classified also regarding the number of simultaneous users. They can be dedicated for one user or shared with other users. The number of simultaneous users can be a limited group of persons or a wide population. More, medical devices can be classified into on-time, continuous or discrete data based on the data generation time line.

A great challenge, related to this layer, consists of supporting this wide range of device types in a various scenarios of care needs and settings all in a harmonious network which needs to be end-to-end managed. Vis-à-vis of the heterogeneous landscape of products, many certification organisms propose different security certification schemes to certify medical devices such as: Common Criteria [22] and European cyber-security certification of the European Cyber Security Organization (ECSO) [23]. Devices are tested and certified with different approaches, in different contexts and countries; this makes the comparison or classification of certified devices more difficult.

4.3.2 Network layer

IoMT take advantage of ICT to spread more widely and offer more services. Devices operate in low power modes within noisy and lossy communication channels. Wi-Fi, Bluetooth, Low-Rate Wireless Personal Area Networks (LR-WPANs), Z-wave, Zigbee are popular communication protocols used in IoT networks. RFID tags are used to identify objects. Device connection to the network can be wired or wireless. The mobile security reference architecture reported that devices using cellular network communications and Wi-Fi are more accessible and exposed to attacks than hardwired devices [22].

Securing an IoMT communication is about ensuring confidentiality, integrity and reliability for data transmission over interconnected ecosystems and this is quite broad. Attacks like *DoS/DDoS, Eavesdropping, Man-in-the Middle, Network Intrusion* are typical threats in this layer [24–26]. Since IoT based networks can be composed of a mixture of protocols supported by wired and wireless physical channels, establishing a secure data transfer with abstraction of this mixture seems to be a complex and challenging task. Due to the use of different protocols and technologies, network management and security are hard to fulfill. This heterogeneity makes the whole system vulnerable. The large number of devices that connect and disconnect from the network at multiple times raises security issues like network congestion, lack of authentication, etc., and it also affects resources availability. More, sensitive information can be intercepted from the network especially when using data retrieval techniques between the nodes.

4.3.3 Application layer

E-health applications have different sets of users with different profiles that require various types of access privileges. Any illegal access can have dramatic consequences, so, effective authentication and access control schemes should be applied. For each communication, the user privacy should be ensured. Sometimes, implemented mechanisms might be vulnerable that may lead to data loss and other damages to the users of the system.

The huge amounts of collected data lead to system management problems such as complexity and the need of many resources and complex algorithms. As a consequence, this may result in data loss, system unavailability or performance slow down (Quality of service "QoS" degradation). With regards to software security, hidden vulnerabilities in the development process of applications can be later exploited by attackers and malicious users.

Figure 4 illustrates the IoMT risk landscape regarding the 3 layers architecture of the basic e-health system model.

4.4 Existent security solutions for e-health systems

Setting up a secure and trusted IoMT system to exchange patient's data despite the constrained resources has been addressed by many researchers. Specific solutions have been proposed. Figure 5 illustrates the main techniques and research axes adopted by researchers within this context. Main contributions deal with cryptography-based solutions (by using classic or defining lightweight encryption), authentication and access control schemes, artificial intelligence based solutions (by applying machine and deep learning algorithms for intrusions detection/prevention for

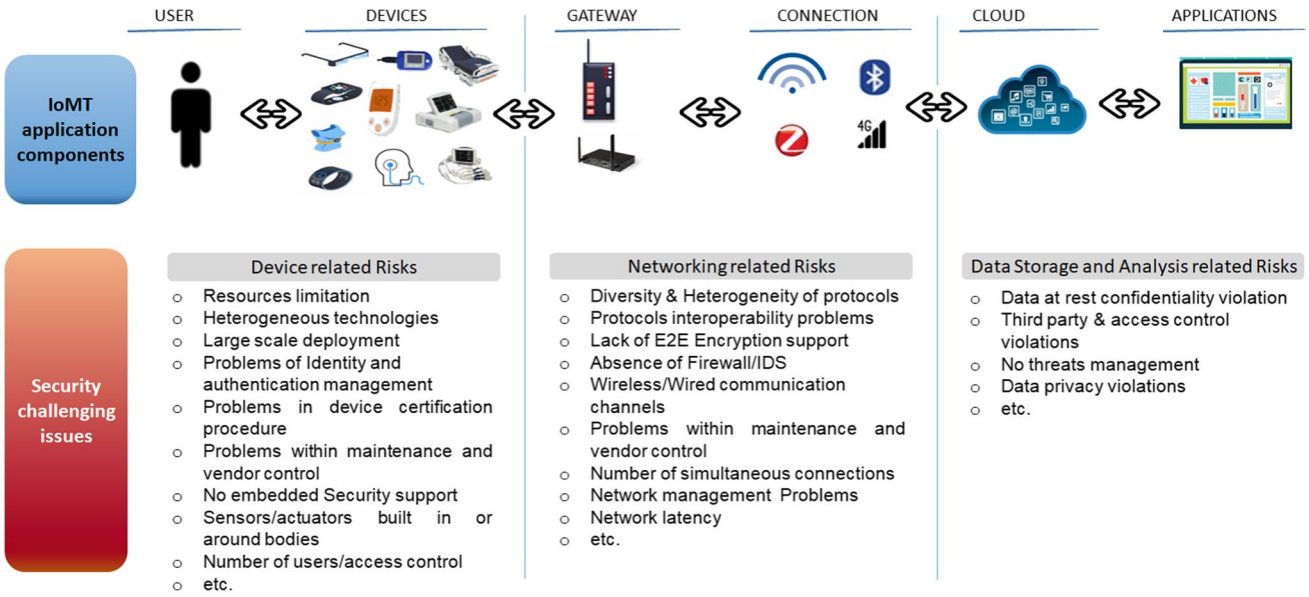

Fig. 4 IoMT risk landscape

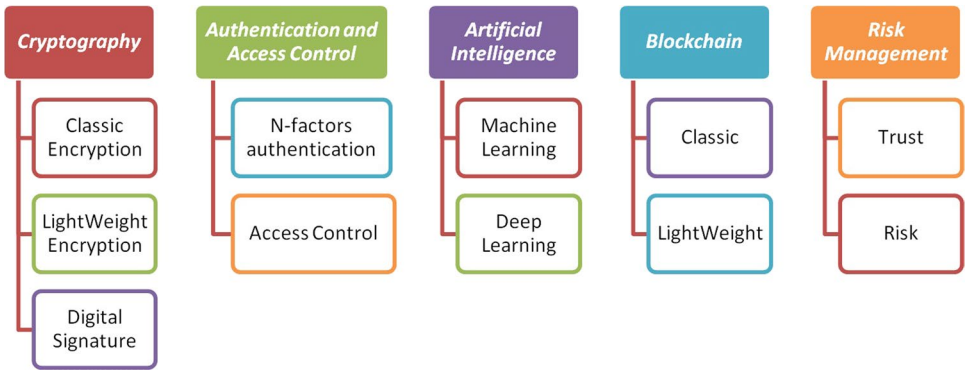

Fig. 5 Security techniques for e-health environments

example), blockchain techniques (classic or lightweight solutions) and risk-trust management frameworks.

In [27], authors studied the performance of several security algorithms, particularly, the implementation of cryptographic algorithms in IoT constrained environments. They compared obtained results to choose the convenient algorithm for a specific device. In the same context, Wang et al. in [28], analyzed Attribute-Based Encryption (ABE) performance in order to determine the best conditions to use ABE in IoT systems. In order to attempt to ensure the security of the entire IoT system rather than a part of it, several secure architectures has been proposed. Authors in [29] propounded a secure architecture for integrated IoT smart-services environment, based on four security levels: user and device authentication, sensor network security, cloud and internet security, applications and services security. This would let users to access applications and services in a protected way. The suggested architecture in [30] is based on the architectural reference model (ARM) and it was designed to deal with the main security and privacy requirements for a smart object during its lifecycle stages. Authors in [31] defined a security architecture which is deployable on mobile e-health platforms. It makes use of electronic personal health records to establish and manage a medication prescription service in mobility contexts. This architecture is supported by RFID technology and it is able to support secure and authenticated interactions. As a weak link chain in an e-health system, Wireless Sensor Network (WSN) gained the attention of many researchers aiming to solve security problems within those networks. In [32], the authors proposed a framework for intrusion prevention in mobile WSN and developed an end-to-end secure routing based on blockchain architecture. The framework takes into account the dynamic structure and the constrained resources of the mobile WSN.

5 Security risk management within e-health systems

5.1 Basic concepts

In order to highlight the importance and usefulness of the risk management for e-health systems, we start with basic definitions to clarify the concepts of risk, risk assessment and risk management as well as the associated dependencies.

Risk The concept of risk is defined according to the International Standardization Organization (ISO) [ISO 31000; ISO 27005] as the effect (positive and/or negative deviation from the expected) of uncertainty on objectives (which can have different aspects such as financial, health, safety, etc.) [33]. In practical cases, it is often expressed as a combination of the consequences, costs or impacts of an event, including changes in circumstances, and the corresponding probability (likelihood) of occurrence.

Security & cyber-security risk In Information System (IS), the security risk corresponds to the risk that occurs due to loss of data, services or systems confidentiality, integrity, or availability, defined as main security requirements. Cyber-security risks are all security risks that can occur within the cyber-space. This kind of risk considers potential adverse impacts to the organization (including assets, mission, functions, image or reputation), users, other organizations, and the country [34].

Risk assessment The risk assessment, according to ISO 31000, is the overall process that consists of risk identification, risk analysis and risk evaluation. Risk identification concerns the listing, recognition and description of hazards and risks factors. Risk analysis is about comprehending hazards nature, determining risk levels and estimating risks. Risk evaluation concerns the comparison of estimated risks against given risk criteria to figure out the risk significance. The assessment may be based on qualitative, quantitative or combined approaches.

Risk management It refers to a set of coordinated activities defined to direct and manage a system, a project or an organization with respect to risk. The security and cyber-security risk management process consists of a range of activities undertaken for protecting data, services and systems from cyber threats such as unauthorized access, in order to: (i) maintain awareness of security and cyber-threats; (ii) identify anomalies, misconfigurations and incidents adversely affecting the system and/or data; and (iii) mitigate the impact of, respond to, and recover from incidents. As illustrated by Fig. 6, the risk management process, according to ISO 31000, consists of systematic application of a set of policies, procedures and practices to the following activities: communication and consultation; context establishment, risk

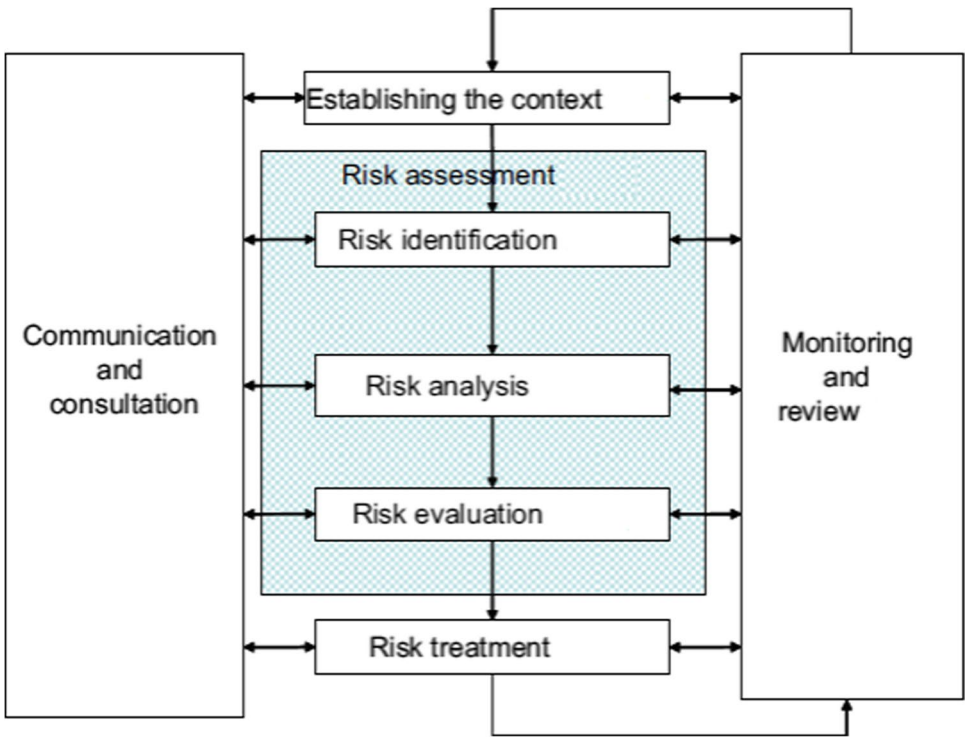

Fig. 6 ISO -Risk management process

assessment (risk identification, analysis and evaluation), risk treatment, risk monitoring and review.

5.2 The trust-risk awareness context

Within trust-risk awareness context, addressing risk management, as highlighted by Fig. 7, deals essentially with two fundamental concepts: the trust and risk concepts. We consider that it is essential to clarify that both of concepts (trust and risk) are highly coupled with each other. Certainly, an object or a system with a low level of trust is seen or considered with a high level of risk and vice versa. Whence considering trust, the main goal is the establishment and evaluation of the trustworthiness of the considered environment. As for the integration of risk awareness in IS, the risk assessment process may follow one of the following analysis approaches: qualitative, quantitative or a combination of both of them. Qualitative approaches are based on qualifying attributes in order to describe potential consequences with their associated occurrence probabilities. In practical cases, by using a qualitative approach, we usually focus on how to mitigate a risk without evaluating its concrete value. Instead of using descriptive attributes, quantitative approaches use numerical values for both consequences and their associated likelihoods. In practical cases, by using a quantitative approach, we usually focus on how to evaluate the value of a risk. In practical cases, when combining both approaches, the qualitative analysis is often used initially in order to obtain a general indication about the risk levels and to figure out the main risks.

5.3 Summary of security risk management solutions for e-health systems

With regards to e-health eco-systems heterogeneity, scalability and complexity, numerous research efforts tackled the e-health risk management thematic from different aspects and points of view. In the current study, we worked to classify related works in three basic categories. First category concerns main risk assessment and management standards, models, frameworks and tools. Second category discusses research works dealing with the incorporation of risk awareness in IoT and IoMT based e-health applications. Third category reviews basic risk management and assessment based access control systems.

For a deeper analysis of major contributions and efforts, we present also a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis of the most relevant proposals. A discussion of related works is then conducted to highlight the limitations of existing solutions and pinpoint the relevance of our contribution.

Trust-risk awareness methods, models and standards Several methods, models, standards and frameworks for trust-risk awareness are defined in literature. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [35] is a method that allows investigating recovery impact areas based on a questionnaire. The TARA method (Threat Assessment & Remediation Analysis) [36], defined as a predictive framework for defending vulnerabilities, allows targeting only most critical exposures. The CVSS (Common Vulnerability Scoring System), defined in [37], computes scores of vulnerabilities severity based on simple mathematical approximations that translate expert's opinions to numerical scores. Exostar, proposed in [38], is a system that

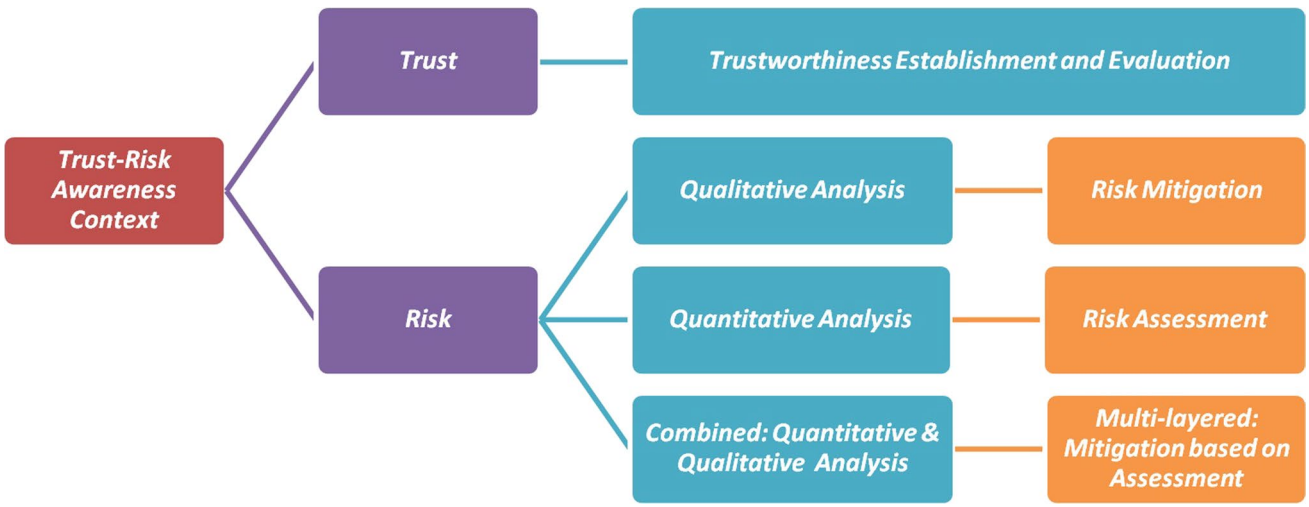

Fig. 7 The trust-risk awareness context

deals with cyber-security of providers or supply chains (it does not evaluate enterprise's stand-alone risk) and regulatory conformity of the supply chain partners. A complementary approach to Exostar is CMMI (Capability Maturity Model Integrated) [39] that deals with stand-alone enterprise risk as well as the risk associated to products development lifecycle. As for standardized models, we present an overview of basic models. The ISO model [33] addresses the standardization (based on consensus) of risk management and assessment. It offers guidelines and standards to help setting up risk management systems but it does not provide mechanisms to guarantee their compliance. The NIST model [34] defines effective and documented processes (as a set of standards and guidelines addressing risk assessment and risk management) that require automation tools and software development to make it of easier utilization. The FAIR (Factor Analysis of Information Risk Institute) model [40] is based on a quantitative approach for the assessment of risk impact. It aims to establish a standard reference which is not based on consensus, but promotes commercial software. As an example of software promoted by FAIR, we cite RiskLens [41] and CyVaR (Cyber Value at Risk) [42]. They are based on quantitative assessment approaches but represent black box tools that may engender standard deviation, consistence and trustworthiness problems.

Trust-risk awareness in IoT, IoMT and e-health Numerous research works addressed the trust and risk assessment in e-health, IoT and IoMT applications. Authors in [43] proposed a quantitative model, based on the coupling of the Cyber-Value-at-Risk (CyVaR) model and the MicroMort (MM) model, for the economic impact assessment of IoT cyber risk. The authors in [44] studied the application of existent security risk assessment approaches and methodologies within an IoT context. They demonstrated that current solutions are not adequate to IoT context due to: shortcomings of periodic assessment, changing systems boundaries, yet limited system knowledge, the challenge of understanding the glue; and failure to consider assets as an attack platform. Hence, the authors highlighted the need for new approaches to assess IoT system risk. In [45], based on the IoT MicroMort model (that adapts to the IoT context both the Cyber-Value-at-Risk model and the MicroMort model), the authors proposed recommendations for performing cyber risk assessment for IoT and better understanding the economic impact of this technology. Authors in [46], dealt with security vulnerabilities identification and mitigation in the context of IoT based on a smart software vendor that lists common vulnerabilities (stored in its database) and provides a possible mitigating solution. In [47], the authors focused on a transformation roadmap for standardizing IoT risk impact assessment (based on functional dependency) and calculating the economic impact of cyber risk (based on a goal oriented approach). Authors in [48], proposed the CSCCRA (Cloud Supply Chain Cyber Risk Assessment) model, as a quantitative risk assessment model to assess the risk of a SaaS application and its supply chain mapping.

Trust-risk awareness in access control Several research works addressed the incorporation of risk awareness within access control systems and particularly role based access control (RBAC) systems. Main contributions focus on four main concepts: (i) enhancing trustworthiness relationships; (ii) defining mitigation strategies based on constraints; (iii) managing accesses based on quantified approaches; or (iv) assessing security policy critical breaches for an efficient and secure policy management. Numerous works proposed to integrate trust relationships in the RBAC model [49–51]. By evaluating the trust levels associated to different components of the policy, only trusted accesses are authorized. Therefore, access decisions are made with regards to components and relationships trust levels. As for the risk mitigation concept, it deals particularly with imposing hard constraints on the policy components in order to tone down associated risks. Several research works dealt with constraints-based risk mitigation approaches and different models have been proposed to formally specify Static Separation of duty (SSoD) and Dynamic Separation of Duty (DSoD) policies [52–55]. More, the authors in [56] proposed to use a mitigation strategy based on risk thresholds and an associated obligation pairs. Concerning the quantification of access risks, the proposed approaches deal mainly with the assessment of risks associated to access requests and authorizing accesses with regards to risk thresholds. To quantify the risk associated to access control, many authors have focused on risk quantification approaches and proposed different frameworks [57–61]. Finally, concerning the management and monitoring of the compliance of access control policies based on risk assessment/management approaches, few works addressed this important thematic. Main contributions focused essentially on the assessment of the risk associated to the policy defects and anomalies [62, 63] as well as the management of policies against attacks scenarios within a correlated anomalies context [64, 65].

5.4 SWOT analysis

Several methods, models and frameworks are encountered in the context of security risk assessment and are motivated diversely. Concerning the risk evaluation techniques, there is no clear limit; both quantitative and qualitative evaluations are used to assess the risk. For a meaningful and conscious impact assessment, various modeling approaches need to be combined or integrated into a new and more reliable model. To better understand the strengths and limitations of existing solutions and to highlight the need for a new comprehensive

Table 1 SWOT analysis of related works

SWOT Proposal	Strengths	Weaknesses	Opportunities	Threats (Risks)
OCTAVE	Generic; investigates recovery impact areas Simplicity; based on a questionnaire	Qualitative; no risk quantification	Applicability; applicable to small companies with limited resources	Complexity; difficult to understand
TARA	Predictive framework	Qualitative; no risk quantification	Complimentary; may be combined with other approaches	Non-exhaustive; targeting only most critical exposures
CVSS	Numerical; translation of experts opinions to vulnerability severity scores	Scoring; only 3 color-coded levels	Scalability; may increase the number of its color-coding system	Truthfulness; relies on a simple mathematical formalism
Exostar	Contextual; supply chain risk assessment	Completeness; ignore standalone risk assessment	Complimentary; may be combined with other approaches	Correctness; depends on a questionnaire that may lead to incorrect results
CMMI	Contextual; enterprise risk and risk in product development lifecycle	Objectivity; detection without correction guidance	Complimentary; complimenting Exostar Updates; related to ISO 9001	Completeness; difficulty to correct identified weaknesses
ISO	Standardization; covers risk assessment and risk management	Compliance; consensus may not be reached or may be non- compliant	Extension; cyber risk assessment	Fairness/Completeness; depends on voluntary compliance and consensus
NIST	Standardization; Extensively; large size and extensive scope	Automation; lack of automation tools and support	Tool supporting;	Complexity; documenting / updates are time-consuming
FAIR	Quantitative; impact assessment that recommends acceptable levels of exposure	Cost; no free tool support	Standardization; without voluntary compliance and consensus	Usefulness; promotes a commercial software
RiskLens	Quantitative; quantitative assessment tool promoted by FAIR	Validation; black box to be trusted without understanding its assessment process	Proof; peer-reviewed process	Confidence; no peer-review validation
CyVaR	Quantitative; quantitative assessment tool promoted by FAIR	Standardization; standard deviation	Extension; different cyber risk assessment	Complexity; difficult to understand
(Radanliev et al. 2018-a) [43]	Quantitative; economic impact assessment of IoT cyber risk	Construction; derived CyVaR and MicroMort weaknesses Automation; no tool support	Standardization;	Complexity; Proof;
(Nurse et al. 2017) [44]	Analysis; discuss the application of existent approaches in IoT context	Completeness; Guidelines	Comprehensive study;	-
(Radanliev et al. 2018-b) [45]	Guidelines; recommendations for IoT cyber risk assessment and understanding its economic impact	Construction; derived CyVaR and MicroMort weaknesses Automation; no tools and support;	Modeling; Implementation;	Complexity; Proof;
(Malik & Singh 2019) [46]	Contextual; vulnerabilities identification and mitigation in IoT context	Basic; based on a smart software vendor	Generalization; Extension; enhanced vulnerability database	Limited; basic lists of common vulnerabilities
(Akinrolabu et al. 2019) [48]	Contextual; cloud supply chain cyber risk assessment	Correlation-free; End-to-end risk;	Extension; different cyber risk assessment	Complexity; Proof;
(Jaidi & Labbene 2015) [62]	Dynamism; dynamic assessment Mixed; quantitative and qualitative assessment	Correlation-free; Contextual; database security policies	Standardization	-

Table 1 (continued)

SWOT Proposal	Strengths	Weaknesses	Opportunities	Threats (Risks)
(Jaidi et al. 2018) [63]	Dynamism; dynamic assessment Mixed; quantitative and qualitative assessment	Correlation-free; End-to-end risk;	Standardization	-
(Cao et al. 2020) [66]	Fine-grained; use of topology attributes	Correlation-free; End-to-end risk;	Standardization	Proof; to be validate in future works

and dynamic approach that takes benefits from existent models, we present, in Table 1, a SWOT analysis of the most relevant reviewed methods, models, approaches, frameworks and systems.

5.5 Discussions

As explained in the previous sections of the current paper, the thematic of security within e-health systems and particularly IoMT applications still remain a challenging aspect. Among other concerning security concepts that need to be enhanced for ensuring the security and preserving the privacy in e-health systems, we focus on the theme of security and cyber-security risk management in IoMT applications. As clearly illustrated by the SWOT analysis, depicted in Table 1, the simple use and direct application of well established risk assessment approaches and methodologies in an IoMT context fails due to several factors (such as context specificities, resource constraints, context dynamism, no standards established yet, high level of surety required, shortcomings of periodic assessment; changing systems boundaries yet limited system knowledge, failure to consider assets as an attack platform; continuous evolution of new and advanced threats, etc.). Therefore, we need new approaches adapted to our context to assess security risks associated to IoMT applications. In this context, recent works addressed mainly the evaluation of the economic impact of IoT cybersecurity threats. Moreover, from the perspective of access control, current solutions failed to manage end-to-end risk and to combine simultaneously both aspects: assessing risks associated to access requests and risks associated to policies critical breaches, anomalies and attacks. In the next section, we introduce a novel dynamic and comprehensive approach to address the discussed limitations of current solutions and respond to new needs related to IoMT security risk management.

6 Security risk management approach within e-health systems

6.1 Designing goals and principle

The e-health environment is mainly characterized by its ubiquity, heterogeneity of devices, diversity of behavior and capability, scarcity of computing resources, changing infrastructures, etc. From the security perspective, it has a wide and complex attack vector/surface since it is under various and continuous changing threat models. Therefore, IoMT applications involve a variety of contexts for managing security risks as well as strategies for risk mitigation which may suit particular cases and do not fit to other cases. Under the above-mentioned risks born out of IoMT, we consider as

evident, the need to identify and build specific risk vectors, factors, attributes, metrics, etc. that are in line with IoMT particularities since those established for traditional systems do not fit exactly main requirements. More, traditional risk management systems are no longer suitable and do not comply with the new requirements.

Setting up a risk assessment process to deal with an IoMT context has to comply with the following basic goals: protecting the data in the originating nodes, ensuring the security of the data when travelling on the communication supports, and preserving the privacy of the system users [67]. To guarantee the effectiveness and the reliability of the IoMT risk management strategy, we define a dynamic and modular risk management approach. The proposed approach relies on the segmentation of the IoMT risk area to smaller zones with particular risk factors. The main objective is to ensure an end-to-end risk assessment. The suggested system divides the whole risk zone to three basic areas: the *DAA*- data acquisition area (associated to the devices), the *DGTA* - data gathering and transmission area (related to network links: LAN, PAN, Wi-Fi, Bluetooth, 2G/3G/4G, etc.) and the *DPSA*- data processing and storage area (typically databases). To ensure a high level and fine-grained risk management, our solution relies on a hybrid (qualitative and quantitative) risk assessment approach. The risk assessment process has to identify the risk vector (threats), establish the set of risk factors and attributes, define the thresholds and the rating method, and determine inherent risks and their associated impacts for the considered IoMT assets.

The main purposes of our proposal are:

- The establishment of a fine-grained risk management process based on the segmentation of the whole risk chain. This process relies on context specific risk metrics, qualifiers, thresholds, factors, ratings, etc.
- The evaluation of the cumulative risk, taking into accounts both inherent and residual risks of the global e-health service delivery chain.
- The automation of the update procedure for risk treatment and risk mitigation response processes.

6.2 System architecture

As illustrated by Fig. 8, our system has a layer-based architecture with a modular structure. We consider three basic sub-systems: DRM (Device Risk Manager), NRM (Network Risk Manager) and SPRM (Storage and Processing Risk Manager). A central unit called orchestrator constitutes the Core unit (Core Risk Manager) of the system.

- *Device Risk Manager (DRM)*:
  Considered as one of the first level decision-makers, this subsystem performs risk management in the context of data acquisition layer. It has its own repository that contains probable risks and risk thresholds related to the devices deployed within the managed IoMT system. The DRM analyses data coming from the generating nodes (devices), evaluates the risk by transforming the input information (risk factors) to quantified risk values based on potential business impacts and likelihoods. The obtained risk value Rd is then compared to a given threshold Td. A risk rate exceeding the predefined threshold involves a risky behavior, countermeasures must be applied. Otherwise, the quantified risk value is transmitted to the core unit for deeper analysis. Logs are also transmitted to the orchestrator for updating its database.
- *Network Risk Manager (NRM)*:
  This subsystem acts also in the first level of decision-making process. Its role is to identify risks related to the communication channels used within the e-health system. This subsystem applies the quantification function to the specific risk factors related to the deployed protocols and communication techniques; obtained risk values are then compared to the predefined threshold (prefixed in the specific database). The communication can be interrupted when a high risk value is obtained. Finally, logs and risk ratings are communicated to the core unit
- *Storage and Processing Risk Manager (SPRM)*:
  It is the third unit in the fine grained risk management framework, related to the data storage and processing subsystem. It performs the same process but with a repository of risk factors related to the databases as an input. Obtained results are also communicated to the Core unit.
- *Core Risk Manager (CRM):*
  This is the central module in charge of performing end-to-end risk management. This unit acts as an orchestrator and is responsible of managing the workflow between the other components. The collected data from the other modules is stored in a global database. Initial thresholds are communicated to the subsystems and are updated regarding the collected results. We can define a periodic update or let the system update thresholds according to the supervised functioning of the system. One of the most important tasks of the CRM is the results correlation.
  This unit updates the elementary databases of the other units if optimized metrics are obtained.

The proposed architecture is based mainly on the elementary modules (DRM, NRM and SPRM) which are autonomous risk agents. They operate and evaluate risks related to each one of the layers and take decisions separately. The Core RM *(CRM)*, as an orchestrator, is responsible for initiating thresholds, storing the results of risk assessment from other modules and building

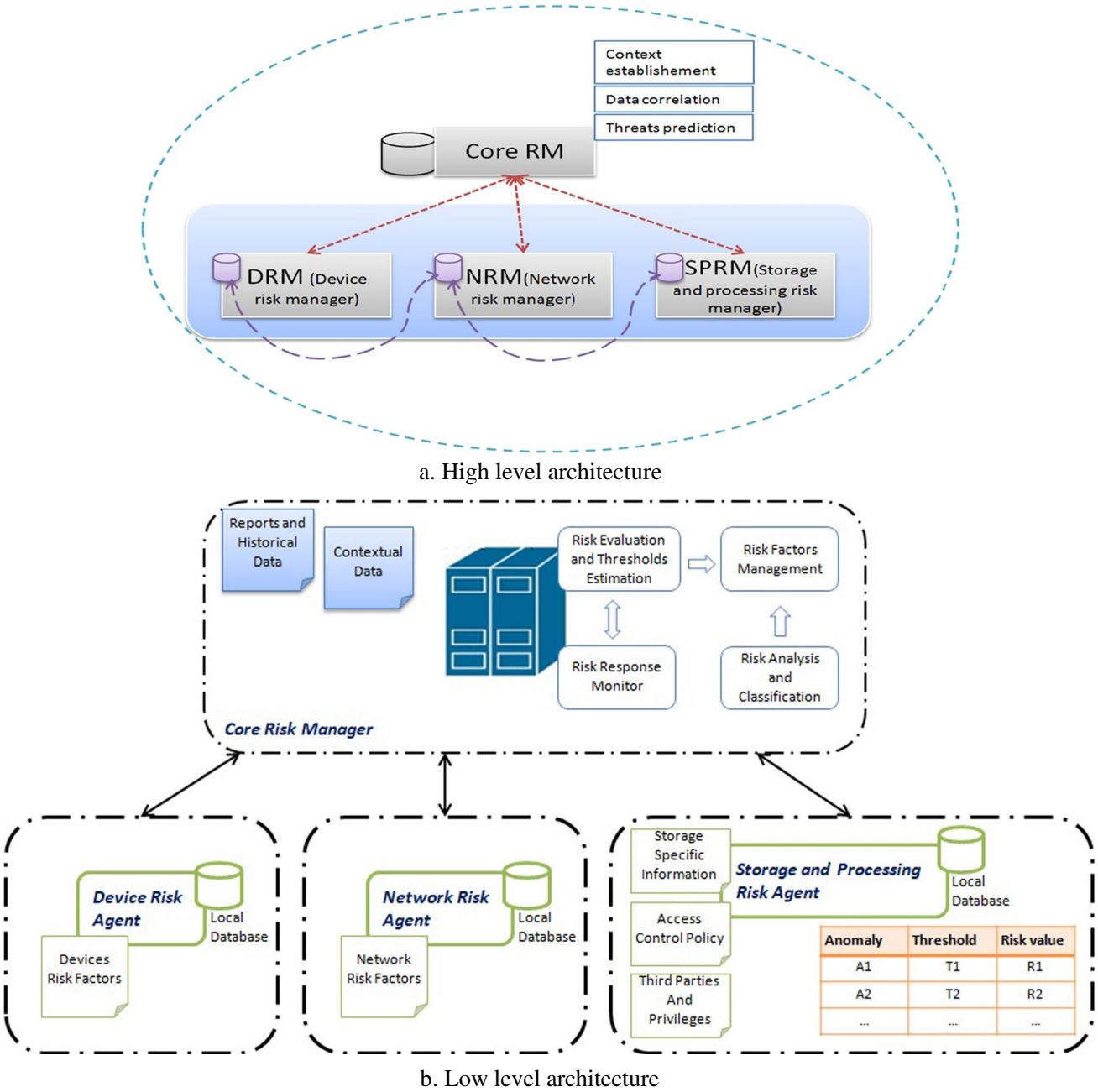

Fig. 8 Dynamic-quantified risk management approach

behavior-based profiles of the system users based on the historical risk rates of the 3 parts. Also, for the non-risky communication scenarios, it logs the risk values to establish historical information about the nodes. So, the CRM supports the other agents and acts like a historical data repository. This module allows a better analysis of the data in order to adjust the thresholds. Hence, the CRM is mainly used to have a centralized vision about the whole system, while the other three modules are capable to autonomously manage the risks in associated area.

IoMT risk management is challenged by many factors. Heterogeneity as a main characteristic of IoMT, involves numerous stakeholders, different types of devices and many protocols for data transmission. Hence the risk management database has to store information about different users (profiles, …), devices (software version, power consumption, support of security features, …), risk thresholds, etc. Information can be gathered from reliable sources like publications of specialized organizations such as CVE (Common Vulnerabilities and Exposures), FDA (Food and Drug Administration), NIST's NVD (National Vulnerability Database) that provide valuable information about security weaknesses and vulnerabilities as well as history of cyber-attacks. Convenient security controls can be also found in these publications. Moreover, providers make technical specifications of their products available for the public that could include indications for supported security features. Databases of risk management should contain all sort of available information concerning the IoMT application.

For the security controls deployed in each part of the system, our framework allows to continuously evaluate their effectiveness depending on the risk rates. In fact, one of the main goals of risk management is to ensure that the impact of realized threats and exploited vulnerabilities is within an acceptable limit. Hence, applying countermeasures aims to reduce this impact and determines how to deal with the risk. The process of assessing risk includes the countermeasures evaluation. In fact, their effectiveness varies when there are changes in the context or the environment where the system being assessed is functioning. For example, increasing password complexity, checking software updates or installing a firewall can be effective actions to mitigate a residual risk but, their effectiveness depends on how they are configured, their impact on the service quality and their cost. The number of stakeholders and their level of security knowledge can impact the effectiveness of security controls in IoMT. So, applying the right countermeasures is a challenging task and a very important step in the process of risk management.

6.3 Risk assessment

In order to take advantages from highly established risk management standards, we followed and adapted to our context the risk management process presented in Section 5 (risk identification, risk analysis and evaluation and risk treatment). Our risk management system is based on the segmentation of the total risk area into three parts: the *DAA*- data acquisition area (associated to the devices), the *DGTA*- data gathering and transmission area (related to network links) and the *DPSA*- data processing and storage area (typically databases). To minimize the system complexity, a specific and autonomous agent is defined for each area and a central agent is responsible of the orchestration between these three parts. Then, in each area, we perform: (i) the identification of the risk vector (threats) and the special risk factors; (ii) the computing of the risk values associated with each abnormal scenario and the evaluation of the cumulative risk of the global e-health service delivery; and (iii) the analysis of the obtained values for classification and automatic treatment (application of countermeasures).

Setting up an efficient risk management process allows slowing down deleterious consequences of an eventual breach and helps with early decision making. Our proposed model for risk assessment is based on a quantified method. Hence, risks are identified, analyzed and assessed separately within different parts of the system properly to the specific context. The global risk assessment method is then applied for evaluating aggregated risk metrics and for a deeper analysis of risk factors. Details about the risk assessment process in our model are described in the following.

Initially, in the CRM, input information are used to identify abnormal scenarios related to the use case such as reports and contextual data, patient and third party users, devices certifications, type of the gateway, countermeasures like redundant data transmission paths, etc. An abnormal scenario (behavior) is any action or request intending to compromise the proper functioning of the system, whether intentionally or accidentally. The proper functioning of the system consists in providing the desired service to the user while maintaining the security of his data. For example the communication interruption caused by a DoS attack or by a sensor failure is considered as an abnormal scenario, the risk level of this abnormality is high if the patient is receiving life-saving treatment and is considered as minor in case of fitness data collection.

Then, for each abnormality an initial threshold is estimated based on the probability of its occurrence, its impact on the system smooth running and taken security countermeasures. These thresholds are communicated to the three other sub-modules. The central module is responsible of initializing risk thresholds for each elementary module or agent. The initial values are set by the security architect according to possible vulnerabilities and countermeasures deployed at each part of the system. Then, periodically, the risk thresholds are updated and adjusted according to the logs returned by each agent (the part which presents the most unusual functioning will have a different level of risk).

In case of an abnormality (e.g. sensor failure), the *DRM*, *NRM* and *SPRM*, as first level decision makers, compute the risk value of the abnormality A_i according to formula (1); where: Pr (k) denotes the occurrence probability of a particular abnormal usage k; k = {1,..., m}; C (k) corresponds to the cost associated to this abnormal usage and CM is the value associated to existing countermeasures.

$$\mathrm{R(Ai)} = \sum_{k=1}^{m} \Pr(k) * C(k) - CM \quad (1)$$

The obtained risk values are then compared to the stored thresholds, two basic scenarios may occur:

i. If $R(A_i) >= threshold$, then the response monitor reacts by applying given reactions such as interrupting the exchange of data and notifying the user, etc.
ii. If $R(Ai) < threshold$, then the new risk value is shared with the CRM.

At a second level, the CRM updates regularly its risk database with new risk metrics and new scenarios. An engine, defined in the CRM, correlates observed abnormalities in order to unveil possible early detection of security issues and/or mitigation of their associated risks. To evaluate the global risk within the system, the CRM evaluation procedure refers to formula (2):

$$Rs = \frac{\alpha * Rd + \beta * Rsp + \gamma * Rn}{\epsilon} \quad (2)$$

Rs is the risk linked to all possible breaches and abnormalities in the whole use case scenario. *Rd* is the risk assessed for abnormalities revealed in the device (the *DAA* area); *Rn* corresponds to the risk assessed for the abnormalities revealed in network agent (the *DGTA* area); and *Rsp* belongs to the risk assessed within the storage and processing part, like hospital databases, (the *DSPA* area). α, β, γ and ϵ tuning variables, with $\alpha + \beta + \gamma \leq \epsilon$, that enable the security administrator to highlight risk mitigation in a chosen part of the system.

As an illustrative example of the assessment model, we consider an initial risk rating (*Extremely High*: $\geq 80\%$; *High*: $\geq 60\%$ and $< 80\%$; *Moderate*: $\geq 40\%$ and $< 60\%$; *Low*: $\geq 20\%$ and < 40; *Minor*: $\geq 0\%$ and $< 20\%$).

6.4 Cases of application

6.4.1 Patient monitoring

a. General Description

Patient monitoring systems are typical applications in e-healthcare. It is important to keep certain trustworthiness for the system users. As illustrated by Fig. 9, the types of the deployed sensors (sensor1 & sensor2 in this case) are stored in the DRM as well as their capabilities, identities, data storage model (local or on the gateway), etc. a copy of the stored data is sent to the CRM. The NRM database stores information about the WSN and all the connections between the sensors and the gateway, protocols, bandwidth, etc. The SPRM stores information associated to the databases (i.e. access lists, users, profiles).

The core risk manager (CRM) module has a global visibility of the end-to-end system risks. Initially every module has to fulfill its risk repository with risk factors and attributes related to its special context. Then it computes inherent risk value for each probable malicious scenario by applying the risk quantification method. In fact, thresholds values are higher in case of using an actuator in an IoMT communication scenario than the one using "read only" sensors. An initial listing of the vulnerabilities, risk factors, and thresholds is established in the risk management modules databases.

In case of a malicious scenario threatening the privacy and the safety of the patient (for instance exploiting a vulnerability in a device which does not support encryption scheme and configured remotely), the DRM will block it in an early stage of the attack.

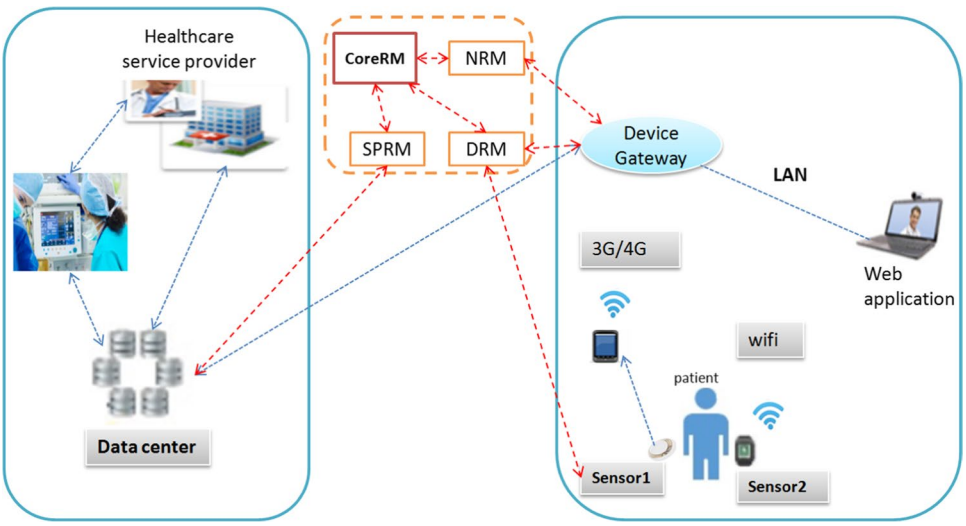

Fig. 9 Patient monitoring general case of study

The risk management framework is based on a fine-grained process using quantified risk metrics. Databases or repositories of risk management subsystems are updated dynamically.

This approach is adaptable to the current context. Its processes require a continuous up-to-date and a fully documented description of the system components. Finally, its architecture makes it flexible in application (due to its modularity) and scalable in order to support wide networks, numerous and heterogonous components. In terms of granularity, it can be extended for a fine-grained assessment for different system components.

b. Application: a Covid-19 monitoring example

Let consider the case, depicted by Fig. 10. Ahmed, as Covid-19 patient, is monitored remotely by a nurse in the health center (hospital). The used smart thermometer allows trucking his temperature and the used electrocardiogram (ECG) allows controlling his cardiac activity. The collected Data is sent (periodically) to the hospital and stored in the system database. The stored measures are analyzed in order to decide about the criticality of the patient health state. Moreover, the smart thermometers measures represent an early warning system about the spreading of the illness within the country [68]. Several kinds of persons could be interested in the gathered data about the pandemic such as researchers, doctors, government organizations or even a simple malicious user who wants to take benefit from the situation. It is clear that due to the high motivation of the breaches initiators, the whole system is under high risks of data violation. More, the user's privacy is also endangered. In case of an emergency situation, the device failover hindered the patient life.

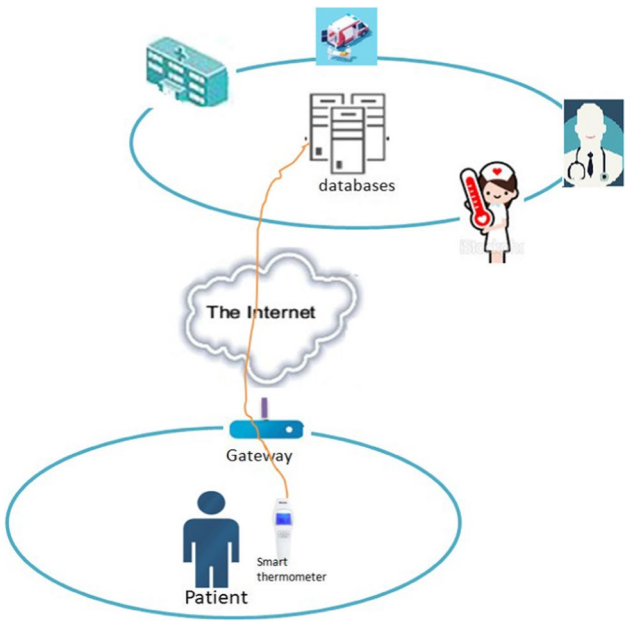

Fig. 10 Covid-19 Patient Monitoring high level architecture

As examples of abnormal scenarios engendered by this application, we cite the following abnormalities: (A_1) Bad temperature metrics, (A_2) No measures reported and (A_3) Non coherent temperature and ECG measures. The risk associated to A_1 is evaluated, according to the previously defined formulas, to*: 70%* by the DRM*, 45%* by the NRM*, 20%* by the SPRM and a global risk of *61.66%* classified as a *High risk*. The risk associated to A_2 is evaluated to*: 80%* by the DRM*, 87%* by the NRM*, 35%* by the SPRM and a global risk of *80.33%* classified as an *Extremely High risk*. The risk associated to A_3 is evaluated to*: 65%* by the DRM*, 45%* by the NRM*, 20%* by the SPRM and a global risk of *57.91%* classified as a *Moderate risk*.

6.4.2 Use case 2: Storage and Processing Risk Manager (SPRM)

The SPRM allows computing the risk values associated to non-compliance anomalies or attack scenarios within storage entities (databases). The SPRM is defined to deal with relational databases as storage entities and also with cloud databases (as a main extension of our previous approach discussed in [62]). First, we consider the evaluation of the risk values associated to non-compliance anomalies relative to RBAC policies within relational databases. The SPRM is composed of the following main components. A *Risk Assessment Engine (RAE)* is responsible of the risk assessment of identified anomalies and threats as well as the estimation/re-estimation of the risk rating and thresholds definition regarding a set of risk factors. A *Response Monitor (RM)* is responsible for analyzing and classifying obtained risk values with respect to corresponding thresholds and ratings. Based on this classification and other parameters, the *RM* may react autonomously vis-à-vis risky situations via blocking access, deactivating privileges, while in normal cases it simply delegates the decision to the CRM, as the core manager, where other actions might be done (i.e. thresholds update). A *Risk Depository (RD)* stores for each case all the required metrics (risk values, risk ratings, risk thresholds, etc.). A *Risk Factors Depository (RFD)* stores a collection of established risk factors (such as context factors, history events, etc.) used for a dynamic evaluation of the risk metrics in addition to an analysis and classification of the defects and attacks. A *Risk Factors Monitor (RFM)* is responsible for managing the stored risk factors, obtained results from risk assessment mechanism and analysis processes, etc.

The *RAE* evaluates the risk of the permission *Pi* according to formulas (3), where *Pr(k)* denotes the probability of occurrence of a particular malicious usage *k; k={1,..., m}*;

C(k) is the cost associated to this malicious usage, and *CM* is the value associated to existing countermeasures.

$$R(Pi) = \sum_{k=1}^{m} Pr\,(k) * C(k) - CM. \quad (3)$$

Therefore, the risk of the role *Rj* is evaluated, according to formula (4), as the sum of the risk values of all permissions assigned to it, where *APR (Rj)* is the set of permissions assigned to *Rj*. Also, The risk of the user *Ui* is computed, via formula (5), as the sum of the risk values of roles assigned to that user noted *AUR(Ui)*.

$$R(Rj) = \sum_{i=0}^{n} R(Pi) | Pi \in APR(Rj) \quad (4)$$

$$R(Ui) = \sum_{j=0}^{n} R(Rj) | Rj \in AUR(Ui) \quad (5)$$

To assess the risk of the access control policy defects, we look for determining the impact/effect of each abnormality on the system, in other words we worked to quantify the effect and influence of identified security breaches on the system. For this, we assess the anomaly risk, according to formula (6), as the ratio between the anomaly sub-elements risk values and the system elements risk values where the selected elements are from the same type.

$$R(Anomaly) = \frac{\sum_{j=0}^{n} R(x) | x \in \{Anomaly\}}{\sum_{l=0}^{m} R(y) | y \in System} * 100\% \quad (6)$$

Obtained results from application in a real world context, the medical system application introduced in [69], highlight the effectiveness as well as the usefulness of the SPRM subsystem. The functional scheme of this application defines two entities: patients and medical records. Every medical record corresponds to exactly one patient and its content stores confidential data whose integrity must be preserved. The security scheme of this example defines five users, two nurses: Alice and Bob, two doctors: Charlie and David and a secretary: Paul. The medical staff contains doctors and nurses. Figure 11 describes the components of the system. It depicts the different actors and their corresponding privileges.

After considering a set of alterations and attack scenarios emphasized by the implemented access control policy when it has evolved to a new state where significant changes are introduced [69]. Via analyzing the vector of attacks, the approach has to identify different cases of non-compliance anomalies. The technical definition of the validation properties and the formal validation process are not under the scope of the current paper.

In order to simplify the evaluation process of the risk values linked to the detected scenarios of anomalies, we: adopted the initial risk rating for classifying the identified anomalies, considered the permission "*modify a medical record*" as the highest risky permission within the system with a risk value evaluated to 8 in a scale that varies from 0 to 10 while the risk values of the rest of the defined permissions are evaluated to 1 in the same scale, and finally considered the "*High Risk*" rating as the risk threshold associated to different anomalies. Our risk assessment process evaluates and classifies the risk values associated to the identified anomalies.

As a scenario of attack, we consider a secretary as a member of the medical staff (i.e. introducing a new hidden hierarchy, called *HARR* in [69], between the roles *Secretary* and *Medicalstaff*). The assessment process considers that *R(**HARR**) = (0.5*100) / (0.5 + 0.1) = 83.33%; (**Extremely High risk**)*. The RM detects an *extremely high risk* related to the hidden assignment of the role *MedicalStaff* to the role *Secretary*. This is normal, since a secretary should not be a member of the medical staff and should not have the right to access to patients private data.

6.5 Discussion and perspectives

Actually, e-health systems still offer neither strong controls for ensuring the security and preserving the privacy of patients nor clear documentation to notify users about inherent and residual risks when specific applications are deployed. Several research works focused on security issues of IoMT systems. It was noticed that they face many challenges. IoMT are resource constrained compared to conventional applications based on electronic devices and ICT infrastructures. In fact, the challenge is about re-architecting

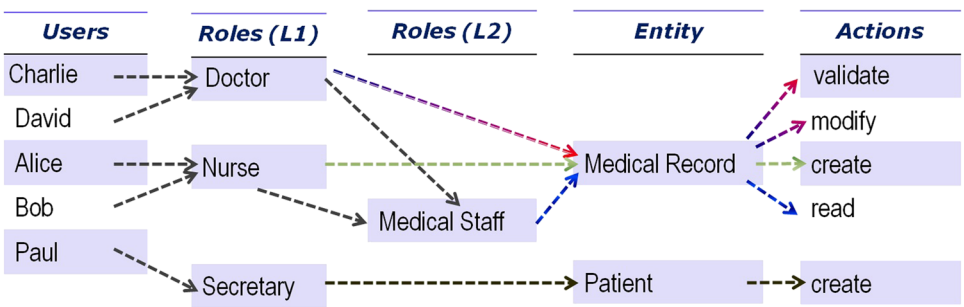

Fig. 11 Description of the medical system application

security solutions to suit the emerging applications and use cases in the e-health paradigms.

We believe that the proposed approach which aims to offer a method for risk management in e-health systems may improve the security and privacy of IoMT infrastructures and minimize the costs associated with the collateral damage that would affect the system's users. The main goals are evaluating and predicting risk damages, identifying new or unseen threats and finally helping the security architects to implement countermeasures for risks mitigation. The framework is based on a cyclical risk management process, dynamic security monitoring, predictive analytics, fine-grained automatic decision-making and updated metrics. This approach is adaptable to the context of IoMT applications. Their processes require a continuous update and a fully documented description of the system components. Finally, its architecture is flexible due to its module-based structure. In terms of granularity, it can be extended to a more fine-grained model by adding other risk agents where needed or if the risk area is too large or complex.

The problem of false/positive attacks is a crucial aspect in such a system. Certainly, we cannot predict all false positive and false negative scenarios. The analysis and correlation between the different log files and the action on risk factors can help mitigating the problem of false positives. Actually, in a first step, we use the tuning coefficients α, β, ϵ and ε to be able to focus on one of the system parts. Risk ratings are adjusted and thresholds are updated to suit the context, but lowering of thresholds to eliminate false positives is likely to lead to false negatives. Data analysis makes future risk more accurate. Whence there is a problem to be investigated (i.e. false positive case), we start by tuning the defined coefficients then, countermeasures are implemented or reviewed.

In a second step (as a perspective), we plan in a future work, to define a smart management approach (based on artificial intelligence techniques for a better and proper analysis of log files) to monitor the proper functioning of the system and particularly reduce false negative/positive attacks.

7 Conclusion

This research work presents a comprehensive study of the e-health systems, in terms of architecture, applications and different challenges, notably, security challenges. In fact, IoMT applications are extremely vulnerable to security threats due to data sensitivity and privacy, fast changing contexts, multitude of stakeholders and old ICT infrastructure. New risk stack arises with these applications deployment. In this manuscript, we detailed the risk landscape related to the heterogeneous components of an IoMT network and then, a critical analysis was presented through the lens of risk methods and frameworks. Most popular risk management approaches are discussed; their IoT risk considerations are explained in terms of strengths and weaknesses. Based on this analysis, we designed a fine grained approach for risk quantification in IoMT contexts. The suggested risk manager is composed of three distributed and chained agents and an orchestrator module. The proposal aims to evaluate risks related to three vulnerable areas in the e-health system: devices zone where data is generated, network area where data is transferred over a multi-node transmission systems and storage infrastructure consisting typically of databases. We aim by our proposal to trigger more investigations in the field of IoMT risks. As a future work, we project to define a smart management approach based on artificial intelligence techniques to monitor the proper functioning of the system.

References

1. BeraA (2019) 80 insightful internet of things statistics (Infographic). Available at: https://safeatlast.co/blog/iot-statistics/. Accessed 20 June 2020
2. Mckinsey (2019) Digital ecosystems for insurers: opportunities through the Internet of Things. Available at: https://www.mckinsey.com/industries/financial-services/our-insights. Accessed 20 June 2020
3. Marketsandmarkets (2020) IoT in healthcare market. Available at: https://www.marketsandmarkets.com/Market-Reports/iot-healthcare-market. Accessed 20 June 2020
4. Mckinsey (2018) The Internet of Things: How to capture the value of IoT. Available at: https://www.mckinsey.com/~/media/McKinsey/How-to-capture-the-value-of-IoT.pdf. Accessed 20 June 2020
5. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor 17(4):2347–2376
6. World Health Organization (2005) Fifty-eighth World Health Assembly: resolutions and decisions, annex. InFifty-eighth World Health Assembly, Geneva, 16–25 may 2005, pp 143–143. Available at: apps.who.int/gb/or/e/e_wha58r1.html. Accessed 29 June 2020
7. Hanson Z (2015) 7 Major challenges facing ehealth. https://www.hansonzandi.com/7-major-challenges-facing-ehealth/. Accessed 29 June 2020
8. De Michele R, Furini M (2019) Iot healthcare: Benefits, issues and challenges. In: Proceedings of the 5th EAI international conference on smart objects and technologies for social good, pp 160–164
9. Abolade TO, Durosinmi AE (2018) The Benefits and challenges of e-health applications in developing nations: a review. Proceedings of the 14th iSTEAMS international multidisciplinary conference, Nigeria, vol 14, pp 37–44
10. Islam SR, Kwak D, Kabir MH, Hossain M, Kwak KS (2015) The internet of things for health care: a comprehensive survey. IEEE Access 3:678–708
11. Asghar MH, Negi A, Mohammadzadeh N (2015) Principle application and vision in Internet of Things (IoT). In: International conference on computing, communication & automation. IEEE, pp 427–431
12. Fadilpašić S (2019) IoT being harmed by lack of security skills. ITProPortal Magazine. https://www.itproportal.com/news/iot-being-harmed-by-lack-of-security-skills/. Accessed 05 July 2020

13. Williams PA, Woodward AJ (2015) Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices (Auckland, NZ) 8:305
14. Healey J, Pollard N, Woods B (2015) The healthcare Internet of things: rewards and risks. Atlantic Council
15. Ayala L (2016) Cybersecurity for hospitals and healthcare facilities: A guide to detection and prevention. Apress, New York
16. Skierka IM (2018) The governance of safety and security risks in connected healthcare. Living in the Internet of Things: Cybersecurity of the IoT - 2018 London 2018:1–12
17. Evesti A, Suomalainen J, Savola R (2014) Security aspects of short-range wireless communication-risk analysis for the healthcare application. Int J Intell Comput Res 5(3/4):438–449
18. Boeckl K, Boeckl K, Fagan M, Fisher W, Lefkovitz N, Megas KN, ... Scarfone K (2019) Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks. US Department of Commerce, National Institute of Standards and Technology
19. Baker F, et al (2016) "Internet of Things (IoT) Security and Privacy Recommendations," Broadband internet technical advisory group. https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php. Accessed 20 May 2020
20. Al-Issa Y, Ottom MA, Tamrawi A (2019) eHealth cloud security challenges: a survey. J Healthc Eng, 2019
21. Hiremath S, Yang G, Mankodiya K (2014) Wearable Internet of Things. Wireless mobile communication and healthcare (Mobihealth), 2014 EAI 4th International Conference on: 304–307
22. Common criteria, Security assurance requirements, Available at: https://www.commoncriteriaportal.org/. Accessed 05 July 2020
23. European Cybersecurity Certification Organization. EU cybersecurity certification framework, Available at: https://www.enisa.europa.eu/topics/standards/certification. Accessed 05 July 2020
24. Yang Z, Yue Y, Yang Y, Peng Y, Wang X, Liu W (2011) Study and application on the architecture and key technologies for IOT. In: 2011 International Conference on Multimedia Technology. IEEE, pp 747–751
25. Wu M, Lu TJ, Ling FY, Sun J, Du HY (2010) Research on the architecture of Internet of Things. In2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol 5. IEEE, pp V5–484
26. Chaqfeh MA, Mohamed N (2012) Challenges in middleware solutions for the internet of things. In: 2012 international conference on collaboration technologies and systems (CTS). IEEE, pp 21–26
27. Khan N, Sakib N, Jerin I, Quader S, Chakrabarty A (2017) Performance analysis of security algorithms for IoT devices. 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC). Dhaka 2017:130–133
28. Wang X, Zhang J, Schooler EM, Ion M (2014) Performance evaluation of attribute-based encryption: Toward data privacy in the IoT. In: 2014 IEEE international conference on communications (ICC). IEEE, pp 725–730
29. Jerald AV, Rabara SA, Bai DP (2016). Secure IoT architecture for integrated smart services environment. In: 2016 3rd international conference on computing for sustainable global development (INDIACom). IEEE, pp 800–805
30. Hernandez-Ramos JL, Bernabé JB, Skarmeta A (2016) Army: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things. IEEE Commun Mag 54(9):28–35
31. Gonçalves F, Macedo J, Nicolau MJ, Santos A (2013) Security architecture for mobile e-health applications in medication control. In: 2013 21st international conference on software, telecommunications and computer networks-(SoftCOM 2013). IEEE, pp 1–8
32. Haseeb K, Islam N, Almogren A, Din IU (2019) Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. Ieee Access 7:185496–185505
33. ISO (2009) International standard: risk management: principles and guidelines. ISO 31000. Principes Et Lignes Directrices. ISO
34. Force JT (2018) Risk management framework for information systems and organizations. NIST Spec Publ 800:37
35. Caralli RA, Stevens JF, Young LR, Wilson WR (2007) Introducing octave allegro: improving the information security risk assessment process. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.
36. Wynn J, Whitmore J, Upton G, Spriggs L, McKinnon D, McInnes R, ... Clausen L (2011) Threat assessment & remediation analysis (tara): Methodology description version 1.0 (No. MTR110176). Mitre Corp Bedford MA
37. CVSS (2017) Common vulnerability scoring system SIG, FIRST. org. Available at: https://www.first.org/cvss/. Accessed 08 July 2020
38. Shaw R, Takanti V, Zullo T, Director M, Llc E (2017) Best practices in cyber supply chain risk management Boeing and Exostar cyber security supply chain risk management interviews. NIST
39. CMMI (2017) What is capability maturity model integration (CMMI). CMMI Institute. Available at: http://cmmiinstitute.com/capability-maturity-model-integration
40. FAIR (2017) Quantitative information risk management | The FAIR Institute. Factor analysis of information risk. Available at: http://www.fairinstitute.org/. Accessed 08 July 2020
41. RiskLens (2017) Risk analytics platform. FAIR Platform Management. [Online]. Available: https://www.risklens.com/platform. Accessed 08 July 2020
42. FAIR (2017) What is a cyber value-at-risk model? Available at: https://www.fairinstitute.org/blog/what-is-a-cyber-undefinedalue-at-risk-model. Accessed 08 July 2020
43. Radanliev P, De Roure DC, Nicolescu R, Huth M, Montalvo RM, Cannady S, Burnap P (2018) Future developments in cyber risk assessment for the internet of things. Comput Ind 102:14–22
44. Nurse JR, Creese S, De Roure D (2017) Security risk assessment in Internet of Things systems. IT Prof 19(5):20–26
45. Radanliev P, De Roure D, Cannady S, Montalvo RM, Nicolescu R, Huth M (2018) Economic impact of IoT cyber risk-analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance. In living in the internet of things: Cybersecurity of the IoT; Institution of Engineering and Technology: London, UK
46. Malik V, Singh S (2019) Security risk management in IoT environment. J Discret Math Sci Cryptogr 22(4):697–709
47. Radanliev P, De Roure DC, Nurse JR, et al (2019) Cyber risk management for the internet of things. https://doi.org/10.20944/preprints2019
48. Akinrolabu O, New S, Martin A (2019) CSCCRA: a novel quantitative risk assessment model for SaaS Cloud Service Providers. Computers 8(3):66
49. Chakraborty S, Ray I (2006) Trustbac: integrating trust relationships into the rbac model for access control in open systems. In: Proceedings of the 11th ACM symposium on access control models and technologies, SACMAT '06, pp 49–58, USA
50. Feng F, Lin C, Peng D, Li J (2008) A trust and context based access control model for distributed systems. In: Proceedings of the 10th IEEE international conference on high performance computing and communications, HPCC '08, pp 629–634, USA
51. Bhargava B, Lilien L (2005) Vulnerabilities and threats in distributed systems. Distributed computing and internet technology. Springer, Berlin Heidelberg, pp 146–157
52. Ferraiolo D, Cugini J, Kuhn R (1995) Role-based access control (RBAC): Features and motivations. In: 11th IEEE annual computer security application conference, pp 241–248

53. Simon RT, Zurko ME (1997) Separation of duty in role based environments. In: Computer Security Foundations Workshop, pp 183–194
54. Gligor V.D, Serban IG, Ferraiolo D (1998) On the formal definition of separation-of-duty policies and their composition. In: 1998 IEEE symposium on security and privacy. IEEE, pp 172–183
55. Jaeger T (1999) On the increasing importance of constraints. In: Fourth ACM workshop on Role-based access control, pp 33–42
56. Chen L, Crampton J (2011) Risk-aware role-based access control. In: Proceedings of the 7th international workshop on security and trust management
57. Cheng P-C, Rohatgi P, Keser C, Karger PA, Wagner GM, Reninger AS (2007) Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In: Security and Privacy, pp 222–230
58. Ni Q, Bertino E, Lobo J (2010) Risk-based access control systems built on fuzzy inferences. ASIACCS '10, pp 250–260, USA
59. Molloy I, Dickens L, Morisset C, Cheng P-C, Lobo J, Russo A (2012) Risk-based security decisions under uncertainty. CODASPY '12
60. Ma J, Adi K, Mejri M, Logrippo L (2010) Risk analysis in access control systems. In: Eighth annual international conference on Privacy Security and Trust (PST), pp 160–166
61. Nissanke N, Khayat EJ (2004) Risk based security analysis of permissions in rbac. In: Proceedings of the 2nd international workshop on security in information systems. INSTICC Press, pp 332–341
62. Jaïdi F, Labbene Ayachi F (2015) A risk awareness approach for monitoring the compliance of RBAC-based policies. In: Proceedings of the 12th international conference on security and cryptography, SECRYPT 2015, pp 454–459
63. Jaïdi F, Labbene Ayachi F, Bouhoula A (2018) A methodology and toolkit for deploying reliable security policies in critical infrastructures. Security and Communication Networks, 2018
64. Evina PA, Ayachi FL, Jaidi F, Bouhoula A (2019). Enforcing a risk assessment approach in access control policies management: analysis, correlation study and model enhancement. In: 2019 15th international wireless communications & mobile computing conference (IWCMC). IEEE, pp 1866–1871
65. Evina PA, Ayachi FL, Jaidi F, Bouhoula A (2018) Anomalies correlation for risk-aware access control enhancement. In: ENASE, pp 299–304
66. Cao Y, Huang Z, Yu Y, Ke C, Wang Z (2020) A topology and risk-aware access control framework for cyber-physical space. Front Comp Sci 14(4):1–16
67. Ksibi S, Jaidi F, Bouhoula A (2020) A comprehensive quantified approach for security risk management in e-health systems. In: Proceedings of the 17th international conference on security and cryptography (SECRYPT 2020), pp 644–649
68. The New York Times (2020) Can smart thermometers track the spread of the coronavirus? Available at: https://www.nytimes.com/2020/03/18/health/coronavirus-fever-thermometers.html. Accessed 08 July 2020
69. Jaïdi F, Labbene-Ayachi F, Bouhoula A (2016) Advanced techniques for deploying reliable and efficient access control: Application to E-healthcare. J Med Syst 40(12):262