Discover Internet of Things

Research

Quality characteristics in IoT systems: learnings from an industry multi case study

Fahed Alkhabbas[1,2] · **Hussan Munir**[1,2] · **Romina Spalazzese**[1,2] · **Paul Davidsson**[1,2]

Received: 4 September 2024 / Accepted: 1 January 2025
Published online: 18 February 2025

Abstract
The Internet of Things (IoT) has transformed our daily life by enabling devices and objects to collect data, communicate, and collaborate to provision novel types of services. Engineering IoT systems is a complex process that should consider a number of quality characteristics to meet the systems' goals. Towards identifying the key quality characteristics of IoT systems, in this study, we conduct semi-structured interviews with seven companies developing IoT solutions within smart energy, smart healthcare, smart surveillance, and smart buildings application areas. The study used the ISO/IEC 25010 model as a reference and a qualitative research approach, i.e., we conducted semi-structured interviews with ten experts and performed content analysis on the data collected from the interviews. The study findings reveal that the ISO/IEC 25010 model does not include the following key quality characteristics that practitioners consider when engineering IoT systems: trust, privacy, and energy consumption. Additionally, we report about trade-offs between quality characteristics, architectural constraints, and challenges related to the achievement of the identified quality characteristics when engineering IoT systems in practice.

Article Highlights

- The ISO/IEC 25010 model does not capture all the core QCs of IoT systems. Specifically, the standard lacks the following core QCs: trust, privacy, energy consumption, and scalability.
- In the studied cases, privacy is always prioritized over other QCs, such as functional suitability, reliability, efficiency, and scalability.
- Most of the reported architectural constraints are about where to process data (e.g., edge or cloud).

Keywords Quality characteristics · IoT · Smart energy · Smart buildings · Smart healthcare · Smart surveillance

1 Introduction

The term Internet of Things (IoT) was proposed by Kevin Ashton in 1999 in the context of supply chain management [1]; however, the definition of the term has evolved over the years and become more inclusive, covering a wide range of applications. IoT is a transformative technology connecting a huge number of physical devices to the internet to enable

✉ Fahed Alkhabbas, fahed.alkhabbas@mau.se; Hussan Munir, hussan.munir@mau.se; Romina Spalazzese, romina.spalazzese@mau.se; Paul Davidsson, paul.davidsson@mau.se | [1]Department of Computer Science and Media Technology, Malmö University, Malmö, Sweden. [2]Sustainable Digitalisation Research Centre, Malmö University, Malmö, Sweden.

data gathering and sharing to interact with the physical world [2–4]. The number of connected IoT devices and objects is projected to reach approximately 75 billion.[1] The data generated by the devices and objects is forecast to reach 79.4 zettabytes (ZBs) by 2025.[2] Some examples of such physical devices and objects include smartphones, cars, motion sensors, cameras, home appliances, grid stations, and even buildings [5]. These IoT systems are designed to collect data from physical devices to automate processes, improve efficiency, and provide new services to the end user. Therefore, the application of IoT systems is not limited to a single domain and can potentially revolutionize various industries, such as education [6], manufacturing [7], health care [8], surveillance [9], energy [10], transportation [11], surveillance [12], entertainment [13], and construction [14, 15], by enabling real-time monitoring and analysis of data from connected devices [16]. The advantages of IoT systems entail improved safety, efficiency, and cost savings. For example, IoT systems can be used to monitor patients remotely and provide real-time data related to patients' health to doctors [8]. In agriculture, the IoT system can be used to access weather conditions to optimize crop yield [17]. In manufacturing, IoT systems can be used to monitor the performance of the equipment and plan for predictive maintenance needs to reduce costs [7]. In the energy sector, an IoT system could be used to maintain the internal temperature of the building to improve energy consumption and reduce costs for the end user [10]. In surveillance, the network camera applications can identify suspicious activities and track targets with unauthorized access [18].

Engineering IoT systems to meet the requirements related to critical quality characteristics is a complex process [19]. The lack of attention to software quality may result in increased cost, security vulnerabilities, and compliance issues [20]. Software quality can be defined as the degree to which a software system meets its specified requirements and fulfills the needs and expectations of its stakeholders [21]. According to the international standard for software quality (ISO/IEC 25010), quality is a multidimensional concept encompassing several aspects, such as functional suitability, performance efficiency, compatibility, interaction capability, reliability, security, maintainability, and portability [22]. The existing quality standards (e.g., ISO/IEC 25010) can be used by engineers to design IoT systems. However, those standards are designed for general software systems and not specifically for IoT systems. Towards bridging this gap, in collaboration with our expert industrial partners, we conducted semi-structured interviews (see Sect. 3.3) to explore the quality characteristics of IoT systems the companies consider while designing these systems. This paper reports practical insights concerning IoT systems' quality characteristics. These quality characteristics include both domain-specific and general quality characteristics of IoT systems. Furthermore, the paper explores the trade-offs between quality characteristics, architectural constraints (e.g., limitations that must be considered when implementing IoT systems), and the challenges companies face in addressing those quality characteristics. The main contributions of the study are stated below.

- **Identification of key quality characteristics:** The study identifies essential quality characteristics for IoT systems across various application areas, including smart energy, healthcare, surveillance, and buildings, using the ISO/IEC 25010 model as a reference framework to guide the identification and analysis of these quality characteristics.
- **Proposal of additional quality characteristics:** The findings suggest that the ISO/IEC 25010 model needs to be complemented with three additional quality characteristics: trust, privacy, and energy consumption.
- **Analysis of trade-offs and constraints:** The study addresses the trade-offs between different quality characteristics, architectural constraints, and the challenges related to achieving certain qualities in IoT systems.

The remainder of this paper is organized as follows: Sect. 2 presents the related work on the quality characteristics of IoT systems; Sect. 3 focuses on research questions and the research method employed to answer the research questions; Sect. 4 discusses the analysis the results based on the data collected from interviews. Finally, Sect. 6 provides a conclusion and outlines future research directions.

2 Related work

Software quality has been considered an essential aspect of software development to evaluate the success of software products since the evolution of software development [21, 23]. It is also important to mention that the terms quality characteristics (QCs) or attribute are used interchangeably in the scientific literature but refer to the same notion of quality characteristics. These quality characteristics are essential for ensuring that IoT systems can provide

[1] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[2] https://www.statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size/.

value to their users and stakeholders in different application areas, such as smart buildings, healthcare, energy, and surveillance.

Ashouri et al. [24] conducted a mapping study to identify the quality characteristics and metrics used to evaluate IoT systems using an edge computing architecture. The analysis shows that performance (e.g., time behavior and resource utilization) is the most frequently used quality characteristic and reported a need for established metrics for quality characteristics such as compatibility, portability, security, and maintainability. Furthermore, the literature needed an in-depth analysis of trade-offs between quality characteristics.

Previous literature has reported the benefits and challenges of IoT systems in designing smart cities. They noted security challenges as the most pressing threat and a greater need for security to protect users' privacy [25, 26]. The proposed mitigation strategies include blockchain technology [27–30], data-driven cyber security [31–33], and a probability-based model [34] for big data security in smart cities. Designing and maintaining the quality of IoT systems pose significant challenges due to the heterogeneous, distributed nature and the integration of the IoT systems with the existing infrastructure. Some of these challenges include interoperability [35], security and privacy [36], scalability [37], energy efficiency [38], and data management [39]. For example, interoperability is a significant hurdle in smart home scenarios involving various devices and communication protocols [35]. Concerning smart IoT energy systems, existing literature highlights important QCs such as reliability, accuracy, data integrity, security, privacy, and energy efficiency for smart IoT energy systems. Estermann et al. [40] explored the role of smart meters in the grid. They highlighted the need for reliability and low latency in executing power limitation commands. Meanwhile, Kim et al. [41] conducted a systematic review of smart energy conservation systems and concluded the need for accuracy and data integrity in energy monitoring systems. Maitra et al.[42] further explored the integration of IoT and blockchain technology to improve portability and reduce energy consumption. Similarly, Firoozjaei et al. [43] presented a hybrid blockchain framework to ensure privacy and trust in energy transactions. The study reported that privacy, security, and reliability are important QCs in energy systems.

Security and privacy have become a paramount concern in the context of healthcare IoT systems, ensuring the confidentiality and privacy of patients' data [36, 44]. Scalability becomes a challenge in IoT systems design and maintenance as the number of devices and data volume continue to grow at an industrial scale [37]. The energy efficiency of IoT devices deployed at remote locations is an issue, given that these devices rely on limited energy sources [38]. Although the data management and analytics capabilities are improving, it is still a significant challenge for edge devices to process and analyze the sheer volume of data generated by IoT devices [39]. Smart healthcare has gained attention in recent years with the emergence of IoT, mobile, and cloud technologies. A study reported five critical characteristics for developing smart healthcare IoT systems. These characteristics include stability, continuity, confidentiality, reliability, and efficiency [45]. Fizza et al. [46] emphasizes the critical role of data quality, response time, transmission rate, stability, accuracy, data completeness, and processing capabilities of IoT systems.

Several studies have been reported to enhance reliability and security in smart surveillance IoT systems. Sicari et al. [47] focused on quantifying these aspects in IoT nodes, emphasizing important quality characteristics such as accuracy and data integrity for real-time surveillance systems. Roman et al. [48] explored various security mechanisms in IoT systems, mentioning the significance of privacy and trust management, which are considered essential for surveillance systems. Data integrity and confidentiality are reported as highly important QCs in surveillance systems. Furthermore, Anagnostopoulos et al. [49] identified key QCs for surveillance systems in IoT-enabled smart campuses. These characteristics include reliability, scalability, accurate detection, data security, and interoperability for integrating heterogeneous devices.

These challenges require a collaborative effort from various stakeholders (e.g., researchers, industry professionals, etc.) to unlock the full potential of IoT systems across industries. Despite the abundance of literature on IoT systems, there appears to be a research gap in identifying quality characteristics specific to the application domain (e.g., smart healthcare, smart energy, and smart buildings). Most existing studies discuss the general quality characteristics of IoT systems, neglecting the importance of domain-specific quality characteristics. This research addresses this gap by interviewing industry professionals from various applications to enhance the understanding of the QCs essential for the development of IoT systems and propose improvements to the existing model.

To summarize, unlike existing work, and based on insights gained from Industry, our study proposes an extension of the ISO/IEC 25010 model with essential QCs that should be considered when engineering IoT systems. Further, we report and discuss trade-offs between IoT systems' QCs and the challenges that practitioners face when engineering IoT systems.

Table 1 Demographic information of interviewees, including role, experience with IoT Systems, and application areas

Interviewee ID	Role	Company	Interview ID	Experience with IoT systems (years)	Application area
I1	Co-Founder & CEO	A	1	11	Smart energy
I2	COO	B		13	Smart energy
I3	Senior consultant	C	2	19	Smart buildings
I4	Product manager	D	3	7	Smart buildings
I5	Senior researcher	E	4	2	Smart buildings
I6	Master Researcher	E		5	Smart buildings
I7	Product manager	D	5	7	Smart healthcare
I8	CEO	F	6	30	Smart healthcare
I9	Line manager	G	7	26	Smart surveillance
I10	Experienced software engineer	G		11	Smart surveillance

3 Research method

This study aims to investigate the quality characteristics of IoT systems from the perspectives of experts in the industry. The research questions formulated for this study are listed in Sect. 3.1. Furthermore, the research method chosen for this study is qualitative, which includes semi-structured interviews with professionals from companies in the field of IoT [50]. The list of semi-structured interviews used during the interview can be found in A. The background information about the context of these companies is explained in Sect. 3.2, and the demographics of the ten interviewee's from the seven companies are presented in Table 1.

3.1 Research questions

The research questions described below, relate to the ISO/IEC 25010 and are based on the research gap presented the above.

RQ1 What quality characteristics are prioritized by the Industry when developing IoT systems?

RQ2 What quality characteristics trade-offs are considered by companies when developing IoT systems in different application areas?

RQ3 What architectural constraints are considered when developing IoT systems within different application areas?

RQ4 What challenges concerning quality characteristics are faced by companies when developing IoT systems in different application areas?

3.2 Case companies and their IoT application areas

We have chosen a multiple-case study design with four different contexts [51]. These contexts included companies from four IoT application areas: smart energy, smart buildings, smart surveillance, and smart healthcare. This study is part of a research collaboration with our industrial partners.[3]. We chose these partner companies because they bring essential industry expertise and resources to develop IoT systems. This collaboration enhances the practical relevance of our research and facilitates knowledge transfer between academia and industry. Furthermore, we selected companies and cases to ensure diversity and multiple perspectives using concrete examples from various application areas. This section provides a brief overview of the context of the case companies chosen for conducting interviews to address the research questions (RQs).

[3] https://mau.se/en/research/projects/intelligenta-och-trovardiga-iot-system/.

3.2.1 Company A

The company specializes in smart energy services and provides a cloud-based infrastructure that unites multiple systems and algorithms to optimize all aspects of the energy system. The set of distinct algorithms supports different sectors, such as buildings and homes. The company develops feasible Original Equipment Manufacturer (OEM) solutions that improve the supply and distribution of district heating. These solutions are branded and marketed to energy firms.

The chosen IoT system is a digital energy ecosystem platform based on a cloud infrastructure. The platform connects stakeholders in the ecosystem, such as energy suppliers, building owners, and algorithm providers, to optimize energy usage and OEM suppliers, such as company B below.

3.2.2 Company B

The company provides heating, cooling, and hot water solutions for various applications. With over 60 years of experience, the company offers different energy options, including conventional and renewable sources. The company's product line includes tap water systems, heating interface units, and district heating and cooling systems, which are manufactured and supported by extensive service expertise. The company's customers include energy companies, installers, facility managers, and local authorities. The chosen IoT system for the interview is a sustainable, efficient, and cost-effective solution for district heating and cooling installed in buildings to maintain the temperature.

3.2.3 Company C

The company offers many products and services worldwide, including cybersecurity, IT consulting, data analytics, and building sustainability and efficiency solutions. With their expertise in building sustainability and efficiency, they offer smart building IoT solutions, including monitoring systems, predictive maintenance, and energy management solutions.

The IoT system selected for the interview is designed to automatically adjust ambient light and temperature in smart rooms based on occupancy status.

3.2.4 Company D

The company is a well-known multinational corporation specializing in advanced technology products and services. Their offerings include various options, such as gaming, music, pictures, electronics, imaging and sensing solutions, financial services, and new initiatives. Some of its latest offerings include smart office and healthcare solutions.

Two *IoT systems* were selected for the interview from company D. The first is a smart office system that automatically predicts the number of people in a room by utilizing sensor data, meeting schedules, and employee locations. The system enables employees to navigate and access the resources they need to complete their tasks.

The second is a smart healthcare system designed to collect health parameters, perform blood analysis, track people both indoors and outdoors, and trigger alarms. The primary customers for this solution are health and rescue companies.

3.2.5 Company E

The company is a global leader in providing innovative solutions for the telecommunications industry and offers a wide range of services and products related to mobile, cloud computing, and IoT solutions. The company uses sensors, data analytics, and connectivity to build sustainable smart cities that enhance citizens' quality of life while reducing costs. The *IoT system* selected for the interview is designed to enhance monitoring, analysis, and optimization of building operations and environments, through exploiting and analyzing real-time data from IoT sensors and devices and the buildings' 3D visualizations.

3.2.6 Company F

The company is dedicated to developing biokinetic algorithms to promote healthy living. After seven years of R&D, it used its expertise in physics and physiology to create these algorithms. The company utilizes a proprietary platform to collect data from diverse sensors, analyze it, and present relevant information to healthcare providers.

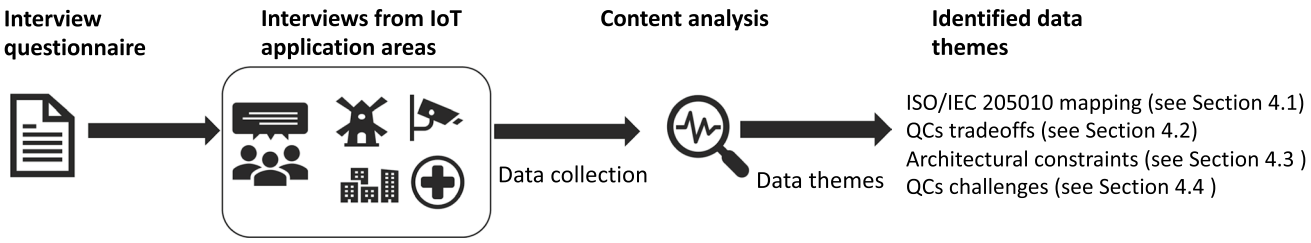

Fig. 1 Data collections and analysis method

The *IoT system* selected for the interview accelerates the rehabilitation of patients with hip fractures through home-based care. Devices and sensors installed on patients collect walking data, detect abnormalities in walking patterns, and notify healthcare providers.

3.2.7 Company G

This company is a global leader in network video and surveillance solutions and plays an important role in shaping the future of video surveillance and communication. The company specializes in developing and producing cutting-edge IP cameras, video encoders, network video recorders, and software solutions. These components form the building blocks of modern video surveillance systems, allowing organizations to monitor, manage, and analyze video data in real-time.

The IoT system chosen for the interview is designed to detect various objects, such as people and vehicles, in data streams and to identify colors using cameras in different contexts, including both indoor and outdoor environments.

3.3 Interviewees selection and data collection

The study utilizes the purposive sampling technique, a non-probability method used to select interviewees from our industrial partners with specific expertise relevant to the IoT systems. [50]. The data collection method chosen in this study is semi-structured interviews (see A), and the interview questions are designed to elicit responses from the participants regarding their experiences of IoT systems and their perspectives on the quality characteristics of these systems. The semi-structured interview questions are developed based on the ISO 25010 Model [4]. on quality characteristics [52]. Each semi-structured interview lasted one hour. The interviewees were selected based on their expertise in developing IoT solutions from application areas such as smart energy, healthcare, surveillance, and buildings. The interviewees' experience in IoT systems provided us with insights on QCs, trade-offs between QCs, and architectural challenges in developing IoT systems. It also helped us identify gaps in the ISO/IEC 25010 model. We have selected the interviewees based on their expertise and availability in IoT systems. We have interviewed seven companies from different application domains, such as smart healthcare, smart buildings, smart surveillance, and smart energy. The interviews were conducted face-to-face and online using Zoom, with the consent of the participants.

3.4 Data analysis method

Figure 1 summarizes the study design and the data analysis method. The study began with a semi-structured questionnaire to ten interviewees from seven companies (see Table 1) concerning IoT systems in the context of smart healthcare, smart energy, smart surveillance, and smart buildings, as shown in Fig. 1. We took notes during the interviews and analyzed the collected qualitative interview data to identify themes in the data by creating an Excel sheet. We utilized a method known as content analysis [53], which involves examining and interpreting data to identify themes in the qualitative data. This process includes coding the notes by highlighting keywords or phrases, grouping similar ideas, and analyzing them to understand common viewpoints or differences among participants. This structured approach helps uncover four underlying themes from the interview notes. These themes include the mapping of QCs to application areas, trade-offs, architecture constraints, and challenges associated with the development of IoT systems. The detailed descriptions of each theme can be found in Sect. 4.

[4] https://iso25000.com/index.php/en/iso-25000-standards/iso-25010.

3.5 Validity threats

This section outlines the validity threats pertaining to the study [54, 55]. We have considered the following validity threats and their mitigation strategies to enhance the research findings on the characteristics of IoT systems.

3.5.1 Internal validity

Internal validity concerns the accuracy and reliability of the study findings [54, 55]. We have considered several internal validity threats, and mitigation strategies were implemented. First, selection bias was recognized as a potential threat, as the interviewees may not represent the larger population of IoT system providers. To address selection bias, a purposive sampling technique was employed, ensuring that interviewees possessed expertise in the field of IoT and had practical experience working with IoT systems. Second, interpretation and confirmation biases were considered by allowing interviewees to select a specific IoT system from their company's context at the beginning of the interview to mitigate preconceived notions from influencing their responses.

3.5.2 External validity

External validity threats relate to the generalizability of research findings to a broader context [54, 55]. In this study, the limited number of interviews may be seen as a threat to the study's external validity. Consequently, the interviewees were selected from diverse companies and various application domains such as smart healthcare, smart office, and smart cities. This approach may improve the generalizability of the results to similar contexts and application areas. Furthermore, the results of this study can be applied to other companies that operate in similar contexts and application areas (see Sect. 3.2). Thus, the external validity of results is limited to the representative companies in sectors such as smart healthcare, smart buildings, smart surveillance, and smart energy.

3.5.3 Reliability

Reliability threats pertain to the consistency and dependability of data and findings [54, 55]. The researchers' biases could have influenced the interview questions, interpretation of responses, and overall data collection process. To address researchers' bias, we created a review protocol document before conducting the study, which all authors reviewed, and multiple interviewers were involved in the data collection process. Furthermore, we have mapped the interview questions on the RQs of the study to ensure that data collection aligns with the study objectives. These measures aimed to minimize individual researchers' biases and enhance the reliability of the study.

3.5.4 Construct validity

Construct validity threats are associated with measuring and operationalizing the constructs under investigation [54, 55]. In this study, an important construct validity threat was the definition of quality characteristics, potentially impacting the study outcomes. The semi-structured interview questionnaire was designed based on the ISO 25010 Model of quality characteristics to address this validity threat. Also, the study clarifies in the related work that the terms quality characteristics and quality attributes have been used interchangeably in the extant literature. Still, both terms comply with the same definition of quality characteristics mentioned in the ISO 25010 Model.

3.5.5 Ethical considerations

This study follows ethical guidelines for research, including obtaining informed consent from the interviewees and ensuring confidentiality and anonymity. Furthermore, all the interview data was handled according to the GDPR guidelines.

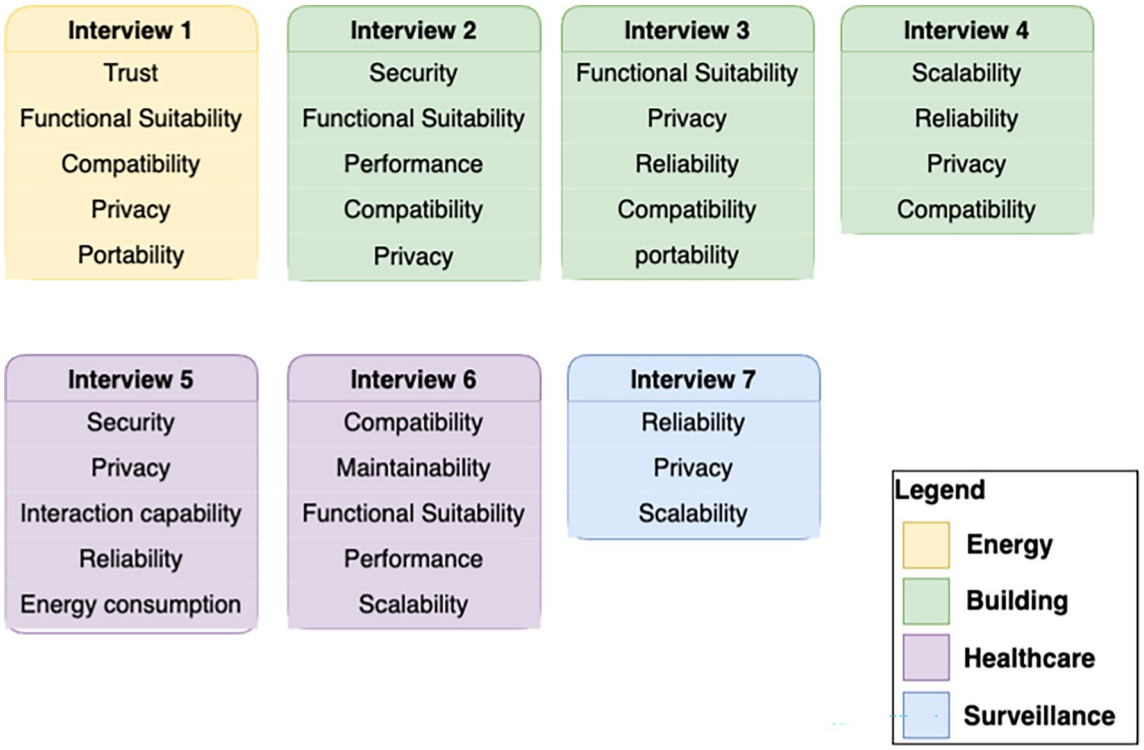

Fig. 2 The quality characteristics reported in the interviews

4 Results and analysis

In this section, we present the findings of our research based on the research questions listed in Sect. 3.1.

4.1 Mapping of quality characteristics to ISO/IEC 25010

This section presents the answer to RQ1 concerning what quality characteristics are prioritized by the industry when developing IoT systems. Specifically, we show how the quality characteristics from different application areas (healthcare, buildings, energy, and surveillance) relate to the ISO/IEC 25010 model (see Figs. 3). Figure 2 shows the quality characteristics reported by the interviewees from all case companies (see Sect. 3.2). The mapping of quality characteristics to the ISO/IEC 25010 model was essential to ensure that our evaluation framework accurately reflects on the essential QCs for practitioners in developing IoT systems. Based on the interviews' data, we identified that trust, privacy, and energy consumption as complementary quality characteristics that the ISO/IEC 25010 model lacks. Therefore, we propose to include them in the ISO/IEC 25010 quality characteristics model. These complementary quality characteristics are shown with the dotted rectangles in Figs. 3 and 4. The extended quality characteristics in the ISO/IEC 25010 model align with the extant literature on trust [56–59], privacy [36, 60–62], and energy consumption [60, 63–66]. These characteristics are well-established terms in the literature and fill critical gaps in the ISO/IEC 25010 standard relevant when engineering IoT systems. Specifically, while security is part of ISO/IEC 25010, it focuses on protection against threats. Whereas privacy refers to protecting the personal and sensitive information collected by the IoT system and complying with regulations [36, 60–62]. Further, while performance efficiency addresses the usage of resources in general, IoT systems uniquely require a focus on energy consumption due to the limited power sources in IoT devices and objects. Finally, privacy, energy consumption, and scalability are at the same granularity level. However, trust is a multifaceted dimension that relates to multiple QCs (e.g., security, privacy, reliability, and performance) [67]. Additionally, it revolves around aspects such as users' confidence in the IoT systems' operations and data integrity. Fig. 4 shows the occurrences distribution of quality characteristics mentioned during the interviews.

Based on the analysis of Fig. 4, it is clear that privacy and compatibility are the most frequently mentioned quality characteristics, with 6 and 5 occurrences, respectively. Besides, reliability and functional suitability have 4 occurrences each,

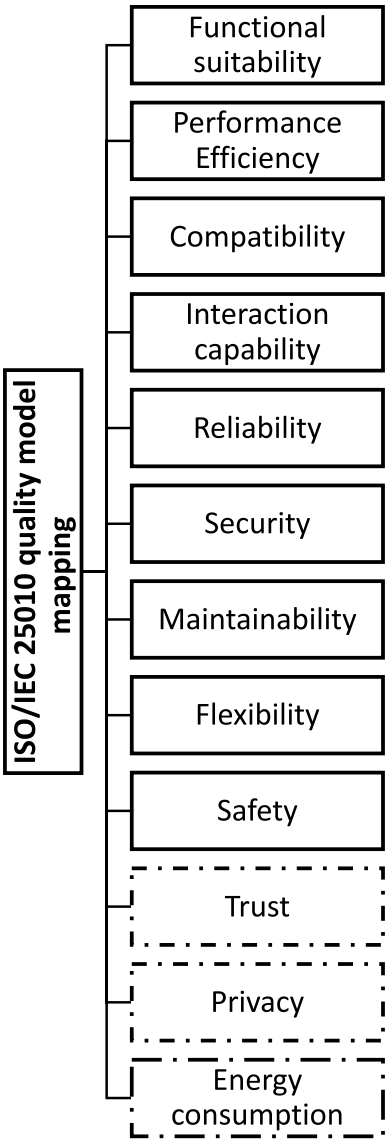

Fig. 3 Quality characteristics mapping to ISO/IEC 25010

while scalability has 3 occurrences. Flexibility, performance efficiency, and security each have 2 occurrences, emphasizing their crucial roles in the adaptability and performance of IoT systems. Finally, maintainability, energy consumption, and interaction capability have only 1 occurrence, possibly indicating their lower priority in the context of IoT systems.

4.1.1 Insights from industry related to the mapping of QCs

This section presents insights from Industry concerning the QCs related to each case company interview and interviewee from various application areas (described in Table 1).

4.1.2 Smart energy systems: insights about the mapping

Company A specializes in smart energy services, providing a cloud-based infrastructure to optimize energy systems. Company B is an OEM provider offering heating, cooling, and hot water solutions for diverse applications.

Both companies work together to provide sustainable heating and cooling solutions through a cloud-based ecosystem. The interviews suggest that functional suitability, compatibility, flexibility, trust and privacy came out as essential quality characteristics for companies A and B. Table 2 shows the industry insights from the two aforementioned case companies. It is also important to highlight that functional suitability [40], compatibility [41], flexibility [42], trust [43]

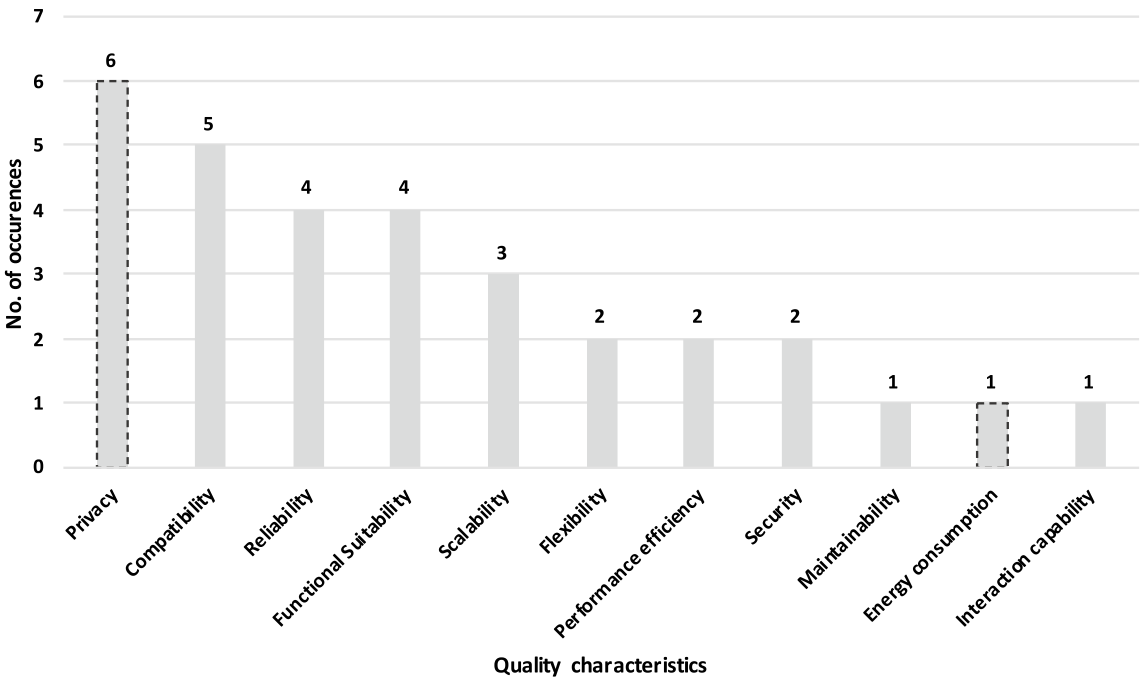

Fig. 4 Occurrences of the identified QCs of IoT systems during the interviews. The dashed bars are the QCs not included in the ISO/ IEC 25010 (trust, not included in the standard, is not shown here since it relates to / involves multiple QCs of the figure)

and privacy [68] are mentioned as essential quality characteristics in the existing literature for the development of smart energy systems. The successful deployment and operation of IoT systems in a smart energy context hinge on several stakeholders. These stakeholders include energy suppliers, building owners, algorithm providers to optimize energy usage, and OEM suppliers.

As indicated by Interviewee I1, the ability to provide functional suitability ensures that the system effectively addresses the dynamic and multifaceted needs of the energy ecosystem without manual intervention. Furthermore, I1 particularly highlighted the significance of compatibility in the face of existing static energy solutions by mentioning: *"For example, connecting OEM devices (e.g., heat pumps, substations, temperature sensors, etc.) and sharing data collected from these devices with other stakeholders such as algorithms providers and energy providers through the energy ecosystem."*

The interview findings highlighted the critical importance of data encryption and local storage in ensuring the confidentiality, integrity, and authenticity of data. Privacy considerations, particularly related to data ownership and GDPR compliance, were emphasized by the interviewees. The implementation of privacy controls, such as clear data ownership definitions, consent mechanisms, and compliance with data protection regulations, have emerged as essential measures to safeguard stakeholders' privacy and trust. Trust is emphasized in multiple instances, ensuring IoT systems' reliability and

Table 2 Insights from case companies A and B in the smart energy industry

QC	Industry insights
Functional suitability	Setting up the system to work automatically without manual intervention
Compatibility	This refers to the compatibility of the current substations with the cloud. The current system is static and needs to become dynamic. For instance, this involves connecting OEM devices (e.g., heat pumps, substations, temperature sensors, etc.) and sharing the data collected from these devices with other stakeholders, like algorithm providers and energy companies, through the energy ecosystem
Flexibility	Integrating hybrid solutions, such as solar power, into the system can help to reduce CO2 emissions
Trust	To ensure that one stakeholder is not optimizing at the expense of another in the system. For example, the use of ventilation and district heating algorithms should be transparent to avoid the unfair prioritization of a particular energy supplier
Privacy	Privacy considerations include data ownership and GDPR compliance for all stakeholders (e.g., energy suppliers, building owners, algorithm providers, OEM suppliers)

transparency amongst all stakeholders. The trustworthiness of the IoT system should ensure that energy optimization should be performed without compromising the stakeholders' interest in the system. Therefore, the ISO 27017 standard is under discussion to establish trustworthiness among stakeholders. As highlighted by I2:

> "Trustworthiness is high on the agenda as the stakeholders need to trust that one stakeholder is not optimizing at the expense of another stakeholder. The company intends to follow the ISO 27017 model by next year to make it more trustworthy for energy suppliers."

4.1.3 Smart buildings: insights about the mapping

Company C, D, and E provide different types of smart building solutions (see Sect. 3.2). In the context of smart buildings, I2, I3, and I4 reported about functional suitability, performance efficiency, compatibility, reliability, security, flexibility, privacy, and scalability as important quality characteristics. Table 4 presents the industry insights about the identified QCs. Our findings are also aligned with the existing literature as the functional suitability [69], performance efficiency [69], compatibility [70], reliability [69], security [69], portability [71], privacy[72] and scalability [73] are mentioned as essential quality characteristics for the development of smart buildings. From the end user's perspective, correct functionality is the most important factor in building trust in the system. Additionally, privacy and security concerns arise when data is transmitted through cloud systems, and firmware updates can pose compatibility issues. Compatibility is a challenge due to the lack of standardization. According to interviewee I3, they "*aim at following the ISO/IEC 25010 to the possible extent*". Maintaining the functional suitability of machine learning models is crucial and requires adaptation to model and data drifts. The cost of the solution, design constraints, and maintainability are essential factors, with input from customers, end users, and facility management organizations.

4.1.4 Smart healthcare: insights about the mapping

Interviewees I7 and I8 mentioned functional suitability, performance, compatibility, interaction capability, reliability, security, maintainability, privacy, energy consumption, and scalability as essential quality characteristics for smart healthcare IoT systems. Table 3 presents the industry insights about the identified QCs.

The findings of these quality characteristics are also confirmed by the existing literature such as functional suitability [74], performance [39], compatibility [75], usability [76], reliability [77], security[77], maintainability, privacy[78], energy consumption [39] and scalability [79].

Based on the interview data, the emphasis on usability, privacy, and energy consumption may be particularly pronounced in smart healthcare due to support for different conditions and disabilities (e.g., touch or button based on one's capabilities), patient data, and the need to charge medical devices. Patients may be reluctant to use the system without user-friendly interfaces. For instance, Interviewee I7 mentioned that "*for energy consumption, the device should not send so much data. There is not much memory for customers to build big applications.*"

4.1.5 Smart surveillance: insights about the mapping

In smart surveillance, I9 and I10 reported about three key QCs: reliability, privacy, and scalability. Table 5 presents the industry insights about the identified QCs.

The aforementioned characteristics are also highlighted in the existing literature of smart surveillance on reliability [80], privacy [81], and scalability [82]. For instance, I9 stated:

> "The devices are located in many different contexts and locations. Thus, the testing should cover all contexts and locations. Detection reliability is important to avoid false detection, especially when alarms are set. Additionally, it is hard to get testing material from the customer side due to GDPR. Thus, it is challenging to run test cases with high accuracy.

Table 3 Insights from case companies F and G in the smart health industry

QC	Industry insights
Functional suitability	I8: comprehensive functionality tests were carried out to make sure that the device achieves its goals
Performance efficiency	I8: falls should be quickly detected
Interaction capability	I7: different versions of the user interface are created to suite a variety of users with different needs. Customers can also create custom interfaces by integrating the capabilities of available sensors and functions
Compatibility	I8: the company manufactured its own device to overcome the compatibility issues of devices in the market
Reliability	I7: the reliability of the device should be tested carefully, also feedback from customers should be collected and analyzed. I8: continuously check components heartbeats and information signals
Security	I7: specialized security teams oversee all development phases, conducting factory reviews, threat analysis, penetration tests, and hacking attempts on both hardware and software. Additionally, a customer's data is encrypted in the device itself and then gets offloaded to the customer's account in the cloud
Privacy	I7: only customers have access to their data and update their devices individually. I8: each patient has a private device and a cloud instance to store his/her data. Thus, patients cannot exchange devices. Additionally, the company complies with GDPR
Scalability	I8: a cloud instance is created for each patient to store and manage her/his data
Energy Consumption	I7: to minimize energy consumption, the device should limit data transmission. Additionally, there is not enough memory for customers to develop large applications
Maintainability	I8: the cost of maintainability was high due to the increase in the cost of chips

Key takeaway
- The ISO/IEC 25010 model does not capture all the core QCs of IoT systems. Specifically, the standard lacks the following core QCs: trust, privacy, and energy consumption.
- Privacy, compatibility, reliability, functional suitability, and scalability are the most influential QCs that drive practitioners' design decisions (please, note that further studies are needed to draw more general conclusions regarding the most important QCs).

4.2 Trade-offs between quality characteristics

Table 6 presents the answer to RQ2 that we collected from practitioners concerning the trade-offs between the QCs (RQ2: What quality characteristics trade-offs are considered by companies when developing IoT systems in different application areas?). Handling such trade-offs is one of the complex steps performed when engineering IoT systems [83]. Ashouri et al. [24] systematically identified that the trade-off between time behavior and resource utilization is the most frequently studied trade-off in the literature concerning the engineering of IoT systems. IoT researchers also studied the trade-offs between resource utilization and functional correctness, and between resource utilization and authenticity.

As can be noted in Table 6, privacy has trade-offs with reliability, functional suitability, efficiency, and scalability. In all the cases, privacy was prioritized over the other QCs. For instance, in the smart surveillance application domain, practitioners decided to process data locally on IoT devices instead of sending it to the server to preserve privacy.

Security is another core QC of IoT systems that was found to have trade-offs with interaction capability and performance. For instance, encryption and decryption of messages affect the performance of IoT systems. Further, the practitioners reported that energy consumption was prioritized over functional suitability to enable devices to run for longer periods.

Table 4 Insights from case companies C, D, and E in the smart buildings industry

QC	Industry insights
Functional suitability	I3: lights should be turned on and temperature Increased in a room only when people enter it. Therefore, sensors' parameters should be Configured properly (e.g., not to detect people passing by the room without entering it)
Performance efficiency	I3: lights should be turned on within a second when a person enters the room. We faced issues where sensors do not detect people in a room and thus the lights in the room remain turned off. Additionally, increasing the temperature requires time, thus, we connected the Temperature adjustment process with the rooms' Booking calendar.
Flexibility	I3: to make it possible to sell the system for different customers, we designed the system using technology that enables the System execution on different platforms over both the edge and the cloud
Compatibility	I3: battery powered things may sleep to optimize energy consumption. During that time, those things become unavailable and do not interoperate with other components. I4, I5, I6: things collect data in different formats and communicate using different protocols. Thus, a middleware is needed To achieve interoperability
Reliability	I4: several factors can affect the accuracy of the ML mModel in detecting the number of people in a room exploiting only sensors' data, including the type of sensors and their placement
Security	I3: a firewall is installed to protect the network from outside attacks. Additionally, things should be protected from unauthorized access (e.g., using keys or credentials). I5, I6: threat identification models and tools should be used to uncover vulnerabilities, especially when offloading data to the cloud
Privacy	I3, I4, I5, I6: available things should not collect Information about people in buildings or their activities
Scalability	I5, I6: deploying software components in a hybrid edge-cloud model supports the scalability of the system

Table 5 Insights from case company G in the smart surveillance industry

QC	Industry insights
Reliability	I9, I10: ensuring reliable detection is crucial to avoid false alarms, especially when alarms are triggered by the detection of specific objects
Privacy	I9, I10: to maintain privacy, the recording of cameras is not streamed to the Cloud. Instead, object detection processes are deployed at the Edge of the network
Scalability	I8: a cloud instance is created for each patient to store and manage her/his data

Table 6 The Trade-offs between the quality characteristics of IoT systems

QC1	QC2	Prioritized QC	Description
Privacy	Functional suitability	Privacy	Excluding the use of devices that provide accurate functionalities due to privacy concerns. For instance, while cameras can accurately detect humans in smart rooms and enable automated lighting, their use is avoided due to privacy concerns.
Privacy	Reliability	Privacy	Excluding the use of devices that provide reliable functionalities due to privacy concerns. For instance, while cameras can accurately count the number of humans in smart rooms, their use is avoided due to privacy concerns.
Privacy	Efficiency	Privacy	Although data can be processed more efficiently in the Cloud, they are processed at the Edge due to privacy concerns. For instance, digitizing dynamic activities in smart buildings requires substantial resources typically available in the cloud. However, due to privacy concerns, resources at the network edge are utilized instead.
Privacy	Scalability	Privacy	Although Cloud resources scale better than the resources at the Edge, data might not be sent to the Cloud due to privacy concerns. For example, digitizing dynamic activities in smart buildings requires computational resources that can auto-scale, which are typically provided by the cloud. However, due to privacy concerns, edge computing resources are used instead.
Security	Interaction capability	It depends on the case	Security measures might affect IoT systems' interaction capability. For instance, complex security configurations can often impact the usability of the system for elderly users.
Security	Performance	It depends on the case	Security requirements might affect IoT systems' performance. For instance, encryption and description of messages affect smart healthcare devices' performance.
Functional suitability	Energy consumption	Energy consumption	Providing accurate results sometimes require IoT devices to run continuously and thus consume more energy. For example, devices designed to monitor patients' mobility must optimize energy consumption to extend battery life, which can impact the accuracy of their functionalities.
Openness	Interaction capability	Openness	Enabling end-users to compose the functionalities of several IoT devices can lead to interaction capability issues. For example, allowing users to create mashups that integrate various IoT devices and services can lead to complex applications with limited interaction capabilities.

Practitioners reported the following aspects that influence their decisions when *prioritizing* the QCs of IoT systems:

1. The design of trustworthy systems. Several companies mentioned that they get feedback from the end-users of their products. Hence, security and privacy were prioritized over other (competing) QCs.
2. Design constraints. For instance, in some cases, engineers were asked not to use their companies' public networks to connect IoT systems. Additionally, to reduce the running costs, they were asked to deploy the software components of the systems on local edge nodes.

Further, the newly identified QCs-trust, privacy, and energy consumption-interconnect with the QCs identified in the ISO/IEC 25010 standard, creating relationships and trade-offs. For instance, trust relates to both security and reliability, as secure and reliable systems improve user confidence in the system. However, implementing strict security measures may incur more energy consumption. Similarly, energy consumption might affect functional suitability, as low-power devices may not support advanced features. Moreover, while prioritizing privacy might enhance user trust, it could

Table 7 The architectural constraints are involved in developing IoT systems

QCs	Constraint	Application domain
Security	To create a specific network to connect IoT devices	Smart buildings
Privacy	To deploy IoT systems' software components and store data on the edge of the network	Smart buildings
	To create independent Cloud instances for different customers	Smart health
Compatibility	The types of devices that could be used at the edge of the network	Smart health, Smart buildings
Energy consumption	Avoid sending all the data via the network	Smart health
	Limit the functionalities that the devices can perform	Smart surveillance
Scalability	To execute processing tasks on the edge of the network	Smart surveillance

reduce systems' performance or increase energy consumption. We plan to investigate more the interconnections and trade-offs between the newly identified QCs and the established ones in the ISO/IEC 25010 standard in our future work.

Key takeaway. We identified trade-offs between multiple QCs. Notably, privacy is always prioritized over other QCs, such as functional suitability, reliability, efficiency, and scalability.

4.3 IoT Systems' Architectural Constraints

Table 7 presents the answer to RQ3 concerning the constraints that practitioners deal with while trying to achieve QCs of the IoT systems they develop (RQ3: What architectural constraints are considered when developing IoT systems within different application areas?). As can be noted, processing and/or storing IoT data at the edge of the network contributes to achieving QCs such as privacy, energy consumption, and scalability.

Note that the reported constraints are related to the specific investigated IoT systems and application domains. This domain-specific focus can limit the generalizability of findings, as the constraints may not apply to different contexts with different requirements. For example, executing and processing tasks on the edge of the network for scalability purposes in the smart surveillance domain might vary in effectiveness depending on infrastructure maturity. Similarly, creating independent Cloud instances for different customers for privacy purposes in the smart health domain might be not possible due to regulations (e.g., GDPR). To improve the generalizability, future research could focus on identifying shared constraints across domains in different contexts by investigating a larger number of systems and developing adaptable strategies that balance domain-specific needs with broder applicability.

Key takeaway. The majority of the reported architectural constraints are about where to process data in the Edge-Cloud continuum. In several application domains, there is an increased data processing trend at the edge (i.e., edge computing) compared to earlier cloud computing. [19, 84].

4.4 The challenges associated with the quality characteristics

Table 8 presents the answer to RQ4 concerning the challenges that practitioners faced while realizing the QCs of the IoT systems they develop (RQ4: What challenges concerning quality characteristics are faced by companies when developing IoT systems in different application areas?). As noted, privacy and reliability-related challenges are reported in most of the IoT application domains. Indeed, it is not possible to verify what data are collected by closed-source devices, where the data is stored, who access it, and for what purposes.

Furthermore, practitioners reported that privacy, security, energy consumption, and scalability are becoming more influential and challenging QCs of IoT systems. Another challenge is to evolve the hardware of IoT devices and systems to cope with the fast evolvement of the software components. Additionally, practitioners foresee the need for more efforts to engineer usable IoT systems that can adapt to support different types of users.

Table 8 The challenges that companies face when realizing IoT systems to meet the desired quality characteristics

QCs	Challenge	Application Domain
Scalability	Connecting a large number of devices to the Cloud and establishing secure communication channels between them	Energy systems
Security	There is a need for tools to perform security-related tests especially on devices' level. It is not easy to verify that a device is secure as claimed in its specifications, especially when the software that runs on devices is not open source	Smart buildings
Privacy	It is hard to verify what data are collected by closed-source devices and who has access to this data when shared with third party (Cloud) platforms	Smart buildings, Smart surveillance, Smart health
	Some users have concerns about their privacy when using the system. Further, it is challenging to collect user data for testing purposes	
Compatibility	There exists no well-adopted standard that allows the interoperability of IoT devices from different brands. A company reported the need to develop their own devices due to interoperability issues. Additionally, sometimes backward compatibility is not maintained during firmware updates	Smart buildings, Smart health
Functional Correctness	It is not always possible to find the root causes of (closed-source) devices' strange behaviors	Smart buildings
Reliability	The machine learning models' performance depends on the training data quality and might degrade due to data and concept drifts	Smart buildings, Smart health, Smart surveillance
Portability	It is challenging to design IoT systems that can adapt to new contexts	Smart buildings Smart surveillance
Performance	Network latency can result with processing errors	Smart buildings
Interaction capability	To design applications that support different categories of users who have different abilities to interact and use IoT systems	Smart health
Energy Consumption	Some IoT devices use batteries that need to be recharged periodically to continue functioning	Smart health

Concerning the intelligent components of IoT systems, engineers reported challenges concerning the collection of data to train and test IoT systems' machine learning models, which affect the systems' reliability in multiple application domains. Additionally, such components should be engineered to adapt to concept and data drifts. Further, those systems should be designed to act autonomously when needed. For instance, surveillance systems should be able to detect intruders automatically and take actions (e.g., triggering alarms and flashlights) without the need to monitor video streams by individuals.

Challenges can also concern multiple QCs. For instance, scalability does not only concern managing a large number of devices but also about maintaining secure communication channels with minimal energy consumption.

Key takeaway. We identified several challenges related to the engineering of IoT systems, spanning across various layers of the IoT stack, from the infrastructure layer to the application layer. Notably, the presence of closed-source devices and systems complicates the process of verifying that IoT systems meet key quality criteria, such as privacy, security, functional correctness, and compatibility.

5 Discussion

In this study, we aimed to investigate different aspects related to the QCs of IoT systems. Specifically, first we investigated whether the ISO/IEC 25010 quality characteristics model is comprehensive and includes all core QCs of IoT systems needed for industrial practitioners while developing their IoT systems in different areas (RQ1). We found that trust, privacy, and energy consumption were essential QCs not explicitly included in the ISO/IEC 25010 model. Therefore, we proposed an extension of the QCs in the ISO/IEC 25010 model, which is aligned with the findings of the extant literature. For instance, several studies have highlighted the importance of trust [43, 56–59, 72, 85], privacy [25, 36, 36, 60–62, 81, 86], and energy consumption [60, 63–66] in IoT systems. The identified QCs are critical across the examined application domains. Specifically, in smart healthcare, the reliability of medical devices and privacy protections for sensitive health data are crucial, while energy-efficient wearables are essential for long-term functionality. Similarly, in smart buildings, systems' reliability, privacy concerns related to occupant data, and energy efficiency are key factors in driving the adoption of sustainable smart buildings. Further, in the case of smart surveillance, ethical considerations and privacy safeguards must be integrated to balance public safety with individual rights, alongside with energy efficiency being essential for continuous operations. Finally, in smart energy, energy-efficiency is a core aspect to ensure net savings. Whereas data accuracy and privacy of consumption patterns are necessary to maintain user trust and comply with regulatory standards (e.g., GDPR.

Further, although the IoT is considered as the fourth wave of digitization and the number of connected devices exceeded fifteen billion,[5] There is still no widely-adopted standard for integrating heterogeneous IoT devices. Hence, compatibility was reported among the most relevant QCs of IoT systems in different application domains. Also, we noted that the companies have their individual metrics for measuring the QCs of IoT systems, and no standard metrics are widely used. Finally, although trust is an important QC of IoT system, there seems to be a lack of common understanding of the dimensions of trust in the IoT. This might be due to the complexity of this QC, as it can be perceived from multiple perspectives, including end-users, managers, engineers, and companies owners. More effort is needed to define trust and engineer trustworthy IoT applications. We plan to address these aspects in our future work.

Secondly, privacy was recognized as the QC that influences practitioners' decisions in most of the application domains. This reveals its role when engineering and deploying IoT systems to meet regulatory requirements (e.g., GDPR) and address ethical concerns in domains like smart healthcare and smart surveillance. Additionally, concerning the trade-offs between IoT systems' QCs, considered when developing them (RQ2), we noted that privacy was prioritized over multiple QCs. This can be due to multiple reasons, including the widespread use of IoT devices and the sensitivity of the data they collect. Further, there is a need for systematic procedures for evaluating IoT systems and handling the trade-offs between them.

Thirdly, practitioners in various application domains seem to face several challenges when trying to achieve the desired QCs of the IoT systems under realization (RQ4). The reported challanges reveal the need for robust infrastructures and reliable protocols to enable large-scale IoT systems. Additionally, there is a systemic lack of transparency and standardization, which affect practitioners ability to validate the security and privacy of closed-source IoT devices.

Finally, the reported architectural constraints (RQ3) indicate that practitioners started using and will use more often edge computing in the future. Additionally, challenges related to network latency (performance) and battery limitations (energy consumption) require IoT specific innovations to address such specific constrains.

Finally, as already mentioned, more studies are needed to draw more general conclusions about the most influential QCs in the different application domains. In this paper, instead, we aimed at eliciting and sharing practical insights about specific cases from the different domains.

6 Conclusions and future work

Identifying, defining, and prioritizing the IoT systems' quality requirements and handling the trade-offs between them are challenging processes. Towards addressing these challenges in this work we aimed at gaining an improved understanding on aspects concerning IoT systems' quality characteristics from practice. We conducted seven interviews with

[5] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

ten expert industrial practitioners from seven companies within four IoT application areas. Our main findings are summarized as follows:

1. The ISO/IEC 25010 model does not capture all the core QCs of IoT systems. Specifically, we propose to extend the ISO/IEC 25010 model to include the following QCs: trust, privacy, and energy consumption. Additionally, we identified and discussed the most relevant QCs of IoT systems in the different application domains.
2. We identified and discussed some trade-offs between a set of QCs.
3. We identified several architectural constraints on IoT systems to meet their QCs.
4. We identified and discussed the challenges practitioners face when realizing IoT systems trying to meet a set of desired QCs.

In our future work, as part of the Synergy project,[6] we plan to investigate the QCs of IoT systems in other application domains. This will include validating the proposed extension of the ISO/IEC 25010 standard and further exploring the trade-offs in various IoT contexts. Moreover, we intend to develop a comprehensive set of specific metrics to rigorously evaluate IoT systems' quality characteristics (QCs) across various applications, including energy, healthcare, buildings, trust, and surveillance. These metrics will help assess the QCs of IoT systems by providing actionable quantitative data to improve the development and efficacy of IoT systems. Furthermore, we plan to critically review the literature to provide a comprehensive overview of the notion of trust for intelligent IoT systems and accordingly propose support models and methods to assess and improve trustworthiness. Finally, we plan to present guidelines and recommendations that would support engineers to incorporate e.g., trust, privacy, and energy consumption considerations, when engineering IoT systems.

Acknowledgements This work was partially funded by the Knowledge Foundation (KK-Stiftelsen) via the project Intelligent and Trustworthy IoT Systems (Grant 20220087).

Author contributions Survey Design: Hussan Munir, Romina Spalazzese, and Paul Davidsson; Planning and Conducting the Interviews: Fahed Alkhabbas, Romina Spalazzese, Hussan Munir, and Paul Davidsson; Data Analysis: Fahed Alkhabbas and Hussan Munir; Writing-original draft preparation: Fahed Alkhabbas and Hussan Munir; Writing-review and editing: Romina Spalazzese and Paul Davidsson; Visualization: Fahed Alkhabbas, Hussan Munir, Romina Spalazzese, and Paul Davidsson.

Data availability All data generated or analyzed during this study are included in this article.

Declarations

Ethics approval and consent to participate All subjects gave informed consent for inclusion before participating in the study. The study was carried out following the national and institutional guidelines, the Declaration of Helsinki (World Medical Association, 2022) and the Swedish Ethical Review Authority (https://etikprovningsmyndigheten.se/wp-content/uploads/2024/05/Guide-to-the-ethical-review_webb.pdf). As the research had no medical background, it involved no risks to our participants. Moreover, the research assessed no sensitive personal data. In consequence, an ethics approval from the Malmö University Ethics Committee was not required.

Competing interests The authors declare no competing interests

[6] https://mau.se/en/research/projects/intelligenta-och-trovardiga-iot-system/.

Appendix

Questions	RQs mapping
What company do you work for?	Demographics
1-1 What products and services the Company offers?	
1-1 What is your role in the organization?	
1-1 How long have you been working in the organization?	
1-1 How many years of experience do you have working with IoT systems?	
1-1 What IoT system do you suggest that we focus on in this interview?	
1-1 How would you describe the IoT system you are working with, and what application area (e.g., smart cars, smart buildings, etc.) does it address?	
What quality characteristics are the most important/prioritized in the development of your IoT system in the company? - Functional suitability (e.g., correctness, completeness, appropriateness) - Performance (e.g., time behavior, resource utilization, capacity) - Compatibility (e.g., co-existence, interoperability) - Useability (e.g., error protection, accessibility, learnability, UI) - Reliability (e.g., availability, fault tolerance, recoverability) - Security (e.g., authenticity, confidentiality, integrity, accountability) - Maintainability (e.g., Modularity, reusability, modifiability, testability) - Portability (e.g., adaptability, installability, replaceability.) - Trust - Privacy	RQ(1,2,3,4)
1-1 Do you follow any software quality model (e.g., ISO/IEC 25,010) in the development of the IoT system in your company?	
1-1 What are the challenges associated with implementing the mentioned quality characteristics?	
1-1 How do you collect quality requirements for the development of the IoT system in your company?	
1-1 Are there any tradeoffs between quality characteristics?	
1-1 What factors contribute to trust and privacy in the IoT system?	
1-1 How do you identify the security vulnerabilities in the IoT system? Could you please share the process (i.e., model)?	
1-1 What tools and methods are most important for assessing the quality of IoT systems?	
1-1 How can the IoT system be designed to be more secure and to protect privacy better?	
What factors impact the choice and prioritization of quality characteristics and metrics?	Other aspects
1-1 Are there any quality attributes that are prioritized when using AI?	
1-1 Are there any Architectural constraints/policies for the company or users of the IoT systems?	
1-1 What trends are emerging in the use of quality characteristics and metrics in the development and assessment of IoT systems in the industry?	
1-1 Do you have any quality characteristics document related to the chosen IoT systems that you could share with us?	
Concluding remarks	

References

1. Ashton K, et al. That 'internet of things' thing. RFID J. 2009;22(7):97–114.
2. Sorri K, Mustafee N, Seppänen M. Revisiting iot definitions: a framework towards comprehensive use. Technol Forecasting Soc Change. 2022;179: 121623.
3. Lesch V, Züfle M, Bauer A, Iffländer L, Krupitzer C, Kounev S. A literature review of iot and cps-what they are, and what they are not. J Syst Softw. 2023;200: 111631.
4. Alkhabbas F, Spalazzese R, Davidsson P. Characterizing internet of things systems through taxonomies: a systematic mapping study. Int Things. 2019;7: 100084.
5. Atzori L, Iera A, Morabito G. The internet of things: a survey. Computer Netw. 2010;54(15):2787–805.
6. Al-Emran M, Malik SI, Al-Kabi M.N.2020. A survey of internet of things (iot) in education: Opportunities and challenges. Toward social internet of things (SIoT) Enabling technologies architectures and applications Emerging technologies for connected and smart social objects. 10: 197–209
7. Mourtzis D, Vlachou E, Milas N. Industrial big data as a result of Iot adoption in manufacturing. Proc cCirp. 2016;55:290–5.
8. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): a vision, architectural elements, and future directions. Future generation computer systems. 2013;29(7):1645–60.

9. Fathy C, Saleh SN. Integrating deep learning-based iot and fog computing with software-defined networking for detecting weapons in video surveillance systems. Sensors. 2022;22(14):5075.
10. Hossein Motlagh N, Mohammadrezaei M, Hunt J, Zakeri B. Internet of things (IoT) and the energy sector. Energies. 2020;13(2):494.
11. Rahim MA, Rahman MA, Rahman MM, Asyhari AT, Bhuiyan MZA, Ramasamy D. Evolution of IoT-enabled connectivity and applications in automotive industry: A review. Vehic Commun. 2021;27: 100285.
12. Santamaria AF, Raimondo P, Tropea M, De Rango F, Aiello C. An IoT surveillance system based on a decentralised architecture. Sensors. 2019;19(6):1469.
13. Hallur GG, Prabhu S, Aslekar A. Entertainment in era of ai, big data & iot. Digital Entertainment: The Next Evolution in Service Sector, 2021;87–109
14. Lam RCY, Junus A, Cheng WMY, Li X, Lam LCH. Iot application in construction and civil engineering works. In: 2017 International Conference on Computational Science and Computational Intelligence (CSCI), 2017;pp. 1320–1325 . IEEE
15. Rajab H, Cinkelr T. Iot based smart cities. In: 2018 International Symposium on Networks, Computers and Communications (ISNCC), 2018;pp. 1–4 . IEEE
16. Sundmaeker H, Guillemin P, Friess P, Woelfflé S, et al. Vision and challenges for realising the internet of things. Cluster Eur Res Projects Int Things Eur Comm. 2010;3(3):34–6.
17. Xu J, Gu B, Tian G. Review of agricultural iot technology. Artificial Intelligence in Agriculture 2022
18. Li S, Kim JG, Han DH, Lee KS. A survey of energy-efficient communication protocols with qos guarantees in wireless multimedia sensor networks. Sensors. 2019;19(1):199.
19. Reggio G, Leotta M, Cerioli M, Spalazzese R, Alkhabbas F. What are iot systems for real? an experts' survey on software engineering aspects. Int Things. 2020;12: 100313.
20. Sowunmi OY, Misra S, Fernandez-Sanz L, Crawford B, Soto R. An empirical evaluation of software quality assurance practices and challenges in a developing country: a comparison of nigeria and turkey. SpringerPlus. 2016;5:1–13.
21. Boehm BW, Brown JR, Lipow M. Quantitative evaluation of software quality. In: Proceedings of the 2nd International Conference on Software Engineering, 1976;pp. 592–605
22. Jung H-W, Kim S-G, Chung C-S. Measuring software product quality: a survey of iso/iec 9126. IEEE Softw. 2004;21(5):88–92.
23. Al-Qutaish RE. Quality models in software engineering literature: an analytical and comparative study. J Am Sci. 2010;6(3):166–75.
24. Ashouri M, Davidsson P, Spalazzese R. Quality attributes in edge computing for the internet of things: a systematic mapping study. Int Things. 2021;13: 100346.
25. Alamer M, Almaiah MA. Cybersecurity in smart city: A systematic mapping study. In: 2021 International Conference on Information Technology (ICIT), 2021;pp. 719–724 . IEEE
26. Mosenia A, Jha NK. A comprehensive study of security of internet-of-things. IEEE Trans Emerg Topics Comput. 2016;5(4):586–602.
27. Chentouf FZ, Bouchkaren S. Blockchain for cybersecurity in IoT in artificial intelligence and blockchain for future cybersecurity applications. Berlin: Springer; 2021.
28. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo K-KR. A systematic literature review of blockchain cyber security. Digital Commun Netw. 2020;6(2):147–56.
29. Abd El-Latif AA, Abd-El-Atty B, Mehmood I, Muhammad K, Venegas-Andraca SE, Peng J. Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in Iot-based smart cities. Inform Process Management. 2021;58(4): 102549.
30. Serrano W. The blockchain random neural network for cybersecure IoT and 5g infrastructure in smart cities. J Netw Computer Appl. 2021;175: 102909.
31. Mohamed N, Al-Jaroodi J, Jawhar I. Opportunities and challenges of data-driven cybersecurity for smart cities. In: 2020 IEEE Systems Security Symposium (SSS), 2020;pp. 1–7 . IEEE
32. Sarker IH. Smart city data science: towards data-driven smart cities with open research issues. Int Things. 2022;19: 100528.
33. Mohamed N, Al-Jaroodi J, Jawhar I, Kesserwan N. Data-driven security for smart city systems: carving a trail. IEEE Access. 2020;8:147211–30.
34. Dattana V, Gupta K, Kush A. A probability based model for big data security in smart city. In: 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), 2019;pp. 1–6 . IEEE
35. Gonzalez-Usach R, Yacchirema D, Julian M, Palau CE. Interoperability in iot. In: Handbook of Research on Big Data and the IoT, 2019;pp. 149–173. IGI Global.
36. Tawalbeh L, Muheidat F, Tawalbeh M, Quwaider M. Iot privacy and security: challenges and solutions. App Sci. 2020;10(12):4102.
37. Sobin C. A survey on architecture, protocols and challenges in Iot. Wireless Personal Commun. 2020;112(3):1383–429.
38. Aliero MS, Qureshi KN, Pasha MF, Ghani I, Yauri RA. Systematic mapping study on energy optimization solutions in smart building structure: opportunities and challenges. Wireless Personal Commun. 2021;119:2017–53.
39. Selvaraj S, Sundaravaradhan S. Challenges and opportunities in IoT healthcare systems: a systematic review. SN Appl Sci. 2020;2(1):139.
40. Estermann T, Springmann E, Köppl S. Method for determining the feasibility of grid and ancillary services through smart meter. Smart Energy. 2021;2: 100018.
41. Kim H, Choi H, Kang H, An J, Yeom S, Hong T. A systematic review of the smart energy conservation system: From smart homes to sustainable smart cities. Renew Sustain Energy Rev. 2021;140: 110755.
42. Maitra S, Yanambaka VP, Puthal D, Abdelgawad A, Yelamarthi K. Integration of internet of things and blockchain toward portability and low-energy consumption. Trans Emerg Telecommun Technol. 2021;32(6):4103.
43. Daghmehchi Firoozjaei M, Ghorbani A, Kim H, Song J. Hy-bridge: a hybrid blockchain for privacy-preserving and trustful energy transactions in internet-of-things platforms. Sensors. 2020;20(3):928.
44. Pandey AK, Das AK, Kumar R, Rodrigues JJ. Secure cyber engineering for IoT-enabled smart healthcare system. IEEE Int Things Magazine. 2024;7(2):70–7.
45. Jeong J-S, Han O, You Y-Y. A design characteristics of smart healthcare system as the IoT application. Indian J Sci Technol. 2016;9(37):52.

46. Fizza K, Banerjee A, Jayaraman PP, Auluck N, Ranjan R, Mitra K, Georgakopoulos D. A survey on evaluating the quality of autonomic internet of things applications. IEEE Commun Surv Tutorials. 2022;25(1):567–90.
47. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in internet of things: the road ahead. Computer Netw. 2015;76:146–64.
48. Roman R, Najera P, Lopez J. Securing the internet of things. Computer. 2011;44(9):51–8.
49. Anagnostopoulos T, Kostakos P, Zaslavsky A, Kantzavelou I, Tsotsolas N, Salmon I, Morley J, Harle R. Challenges and solutions of surveillance systems in IoT-enabled smart campus: a survey. IEEE Access. 2021;9:131926–54.
50. Yin RK. Case study research: design and methods. Thousands oaks: International Educational and Professional Publisher; 1994.
51. Runeson P, Höst M, Rainer A, Regnell B. Case study research in software engineering: guidelines and examples. Hoboken: John Wiley & Sons; 2012.
52. Oriol M, Marco J, Franch X. Quality models for web services: a systematic mapping. Inform Softw Technol. 2014;56(10):1167–82.
53. Cruzes DS, Dybå T. Research synthesis in software engineering: a tertiary study. Inform Softw Technol. 2011;53(5):440–55.
54. Merriam S. What can you tell from an N of 1? Issues of validity and reliability in qualitative research. PAACE J Lifelong Learn. 1995;4:50–60.
55. Gencel C, Petersen K. Worldviews, research methods, and their relationships to validity in empirical software engineering research. In: Proceedings of the International Workshop on Software Measurement (Mensura 2013) 2013.
56. Wei L, Yang Y, Wu J, Long C, Li B. Trust management for internet of things: a comprehensive study. IEEE Int Things J. 2022;9(10):7664–79.
57. Wang J, Yan Z, Wang H, Li T, Pedrycz W. A survey on trust models in heterogeneous networks. IEEE Communications Surveys & Tutorials 2022.
58. Kong W, Li X, Hou L, Yuan J, Gao Y, Yu S. A reliable and efficient task offloading strategy based on multifeedback trust mechanism for IoT edge computing. IEEE Int Things J. 2022;9(15):13927–41.
59. Shirvani MH, Masdari M. A survey study on trust-based security in internet of things: challenges and issues. Int Things. 2022;10: 100640.
60. Chiang M, Zhang T. Fog and IoT: an overview of research opportunities. IEEE Int Things J. 2016;3(6):854–64.
61. Atlam HF, Wills GB. IoT security, privacy, safety and ethics. Digital Twin Technol Smart Cities. 2020;10:123–49.
62. Chanal PM, Kakkasageri MS. Security and privacy in IoT: a survey. Wireless Personal Commun. 2020;115(2):1667–93.
63. Svorobej S, Takako Endo P, Bendechache M, Filelis-Papadopoulos C, Giannoutakis KM, Gravvanis GA, Tzovaras D, Byrne J, Lynn T. Simulating fog and edge computing scenarios: an overview and research challenges. Future Int. 2019;11(3):55.
64. Brady S, Hava A, Perry P, Murphy J, Magoni D, Portillo-Dominguez AO. Towards an emulated iot test environment for anomaly detection using nemu. In: 2017 Global Internet of Things Summit (GIoTS), 2017;pp. 1–6 . IEEE
65. Gupta H, Vahid Dastjerdi A, Ghosh SK, Buyya R, ifogsim. A toolkit for modeling and simulation of resource management techniques in the internet of things edge and fog computing environments. Softw Pract Experience. 2017;47(9):1275–96.
66. Georgiou K, Xavier-de-Souza S, Eder K. The IoT energy challenge: a software perspective. IEEE Embedded Syst Lett. 2017;10(3):53–6.
67. Bekri W, Jmal R, Fourati LC. Secure and trustworthiness IoT systems: investigations and literature review. Telecommun Syst. 2024;85(3):503–38.
68. Tewari A, Gupta BB. Security, privacy and trust of different layers in internet-of-things (IoTs) framework. Future Generation Computer Syst. 2020;108:909–20.
69. Al Dakheel J, Del Pero C, Aste N, Leonforte F. Smart buildings features and key performance indicators: a review. Sustain Cities Soc. 2020;61: 102328.
70. Aguilar L, Peralta S, Mauricio D. Technological architecture for iot smart buildings. In: 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2020;pp. 1–6 . IEEE
71. Jia M, Komeily A, Wang Y, Srinivasan RS. Adopting internet of things for the development of smart buildings: a review of enabling technologies and applications. Automat Constr. 2019;101:111–26.
72. Altaf A, Abbas H, Iqbal F, Khan MMZM, Daneshmand M. Robust, secure, and adaptive trust-oriented service selection in IoT-based smart buildings. IEEE Int Things J. 2020;8(9):7497–509.
73. Png E, Srinivasan S, Bekiroglu K, Chaoyang J, Su R, Poolla K. An internet of things upgrade for smart and scalable heating, ventilation and air-conditioning control in commercial buildings. Appl Energy. 2019;239:408–24.
74. White G, Nallur V, Clarke S. Quality of service approaches in IoT: a systematic mapping. J Syst Softw. 2017;132:186–203.
75. Alshehri F, Muhammad G. A comprehensive survey of the internet of things (IoT) and ai-based smart healthcare. IEEE Access. 2020;9:3660–78.
76. Mutanu L, Gupta K, Gohil J. Leveraging IoT solutions for enhanced health information exchange. Technol Soc. 2022;68: 101882.
77. Ali A, Rahim HA, Pasha MF, Dowsley R, Masud M, Ali J, Baz M. Security, privacy, and reliability in digital healthcare systems using blockchain. Electronics. 2021;10(16):2034.
78. Othman SB, Almalki FA, Chakraborty C, Sakli H. Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies. Computers Electr Eng. 2022;101: 108025.
79. Javed A, Malhi A, Kinnunen T, Främling K. Scalable iot platform for heterogeneous devices in smart environments. IEEE Access. 2020;8:211973–85.
80. Beghdadi A, Asim M, Almaadeed N, Qureshi MA. Towards the design of smart video-surveillance system. In: 2018 NASA/ESA Conference on Adaptive Hardware and Systems (AHS), 2018;pp. 162–167 . IEEE
81. Zhang F, Pan Z, Lu Y. Aiot-enabled smart surveillance for personal data digitalization: contextual personalization-privacy paradox in smart home. Inform Management. 2023;60(2): 103736.
82. Moens P, Bracke V, Soete C, Vanden Hautte S, Nieves Avendano D, Ooijevaar T, Devos S, Volckaert B, Van Hoecke S. Scalable fleet monitoring and visualization for smart machine maintenance and industrial iot applications. Sensors. 2020;20(15):4308.
83. Alkhabbas F, Alsadi M, Alawadi S, Awaysheh FM, Kebande VR, Moghaddam MT. Assert: a blockchain-based architectural approach for engineering secure self-adaptive IoT systems. Sensors. 2022;22(18):6842.

84. Alkhabbas F, Spalazzese R, Cerioli M, Leotta M, Reggio G. On the deployment of iot systems: An industrial survey. In: 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), 2020;pp. 17–24 . IEEE
85. Fritsch L, Groven A-K, Schulz T. On the internet of things, trust is relative. In: Constructing Ambient Intelligence: AmI 2011 Workshops, Amsterdam, The Netherlands, November 16-18, 2011. Revised Selected Papers 2, 2012;pp. 267–273 . Springer
86. Rosner G, Kenneally E. Privacy and the internet of things: Emerging frameworks for policy and design. In: Rosner, Gilad and Kenneally, Erin, Privacy and the Internet of Things: Emerging Frameworks for Policy and Design (June 7, 2018). UC Berkeley Center for Long-Term Cybersecurity/Internet of Things Privacy Forum 2018.