On the Deployment of IoT Systems: An Industrial Survey

Fahed Alkhabbas[†], Romina Spalazzese[†], Maura Cerioli[*], Maurizio Leotta[*], Gianna Reggio[*]
[†]Internet of Things and People Research Center, Malmö University, Sweden
[†]Department of Computer Science and Media Technology, Malmö University, Sweden
{fahed.alkhabbas, romina.spalazzese}@mau.se
[*]Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi (DIBRIS), Università di Genova, Italy
{maura.cerioli, maurizio.leotta, gianna.reggio}@unige.it

***Abstract*—Internet of Things (IoT) systems are complex and multifaceted, and the design of their architectures needs to consider many aspects at a time. Design decisions concern, for instance, the modeling of software components and their interconnections, as well as where to deploy the components within the available hardware infrastructure in the Edge-Cloud continuum. A relevant and challenging task, in this context, is to identify optimal deployment models due to all the different aspects involved, such as extra-functional requirements of the system, heterogeneity of the hardware resources concerning their processing and storage capabilities, and constraints like legal issues and operational cost limits. To gain insights about the deployment decisions concerning IoT systems in practice, and the factors that influence those decisions, we report about an industrial survey we conducted with 66 IoT architects from 18 countries across the world. Each participant filled in a questionnaire that comprises 15 questions. By analyzing the collected data, we have two main findings: (i) architects rely on the Cloud more than the Edge for deploying the software components of IoT systems, in the majority of the IoT application domains; and (ii) the main factors driving deployment decisions are four: reliability, performance, security, and cost.**

***Index Terms*—Industrial Survey; Deployment of IoT Systems; Deployment Decisions Drivers; Edge-Cloud Continuum.**

I. Introduction

The Internet of Things (IoT) technology permeates almost all aspects of our daily lives. The number of connected things is rapidly increasing[1] and IoT applications are widely used in various domains, such as industrial and building automation, health care, transportation, and logistics [5], [23]. Similarly to traditional software systems, designing the architecture of an IoT system encompasses several aspects, including modeling the system's software components and their interconnections, specifying the hardware infrastructure required to host the system, and deciding where to *deploy* the software components within the hardware infrastructure [4], [19].

In general, the software components of IoT systems can be deployed in the Cloud, at the Edge of the network, or across both layers. Designing architectures allowing the optimal deployment of IoT systems is a complex and multifaceted problem that requires the consideration of several aspects, including the following ones. First, the extra-functional requirements that the systems should meet to achieve their goals satisfactorily. Second, the heterogeneity of the processing and storage capabilities of the hardware resources across the Edge and Cloud layers. Those resources also have different properties in terms of response time, availability, privacy, and other quality characteristics. Third, other aspects and constraints, such as legal issues and operational cost limits.

Several methodologies, approaches, and tools have been proposed by the research community to solve the problem of how to deploy an IoT system within a hardware infrastructure. While the majority of those studies aim to solve the problem dynamically at runtime considering a limited number of quality attributes, few works address the issue at design time, aiming at supporting architects to design optimal deployment models [3], [7], [8], [24].

To identify the main drivers for the deployment decisions of IoT systems in practice, we decided to use part of the data obtained by a survey we conducted for *Analysing the State-of-the-practice of the Software Engineering for IoT in the Industry*. For this purpose, we designed and distributed a questionnaire that includes 35 questions and was answered by 444 people (a size comparable to that of other academic surveys, e.g., [20], [26]). More in detail, in this paper, we analyze a subset of the data that includes 15 questions answered by 66 IoT architects from 18 countries across the world.

The *audience* of this study consists of both researchers interested in contributing to the research about the deployment of IoT systems and practitioners who can take advantage of the findings of the study when engineering IoT systems.

The remainder of this paper is organized as follows. Section II discusses related works. Section III describes our research methodology. Section IV presents an overview of the survey participants. Section V reports the findings of the study. Section VI discusses the results. Finally, Section VII concludes the paper and provides future work directions.

II. Related Work

There are few surveys providing insights about aspects related to engineering IoT systems in practice. Kowatsch et al. [18] present the results of a survey about the privacy concerns of IoT systems in the European community. Akbar

[1] https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf

et al. [1] conducted a literature review to identify the risks related to IoT data privacy and security. They validated the findings of the review by conducting an empirical study with IoT practitioners using a questionnaire. The teknowlogy Group[2] run a survey among IoT practitioners aimed to evaluate several aspects of the currently available IoT platforms, such as performance, security, and customer satisfaction.

Several studies address the problem of how to deploy the software components within hardware infrastructures in the Edge-Cloud continuum [7], [21]. The majority of those studies address the issue at runtime by proposing approaches to enable the dynamic deployment of the software components within hardware infrastructures, considering a few factors, typically performance and energy consumption [3], [7]. Other considered factors are the hardware and/or software capabilities of the resources and their workload (e.g., [6], [13], [14]), the size of the data transmitted among the systems constituents (e.g., [27]), the cost (e.g., [9], [15]), and other contextual dimensions, such as mobility of users and devices (e.g., [12], [15]).

Very few works aim at supporting the architects in selecting optimal deployment models at design time. Ashouri et al. [3] consider the relevance of the key quality attributes when making design decisions concerning the deployment of IoT systems and discuss how those attributes can influence the designer decisions. To summarize, the research community has identified several factors that can influence the deployment decisions concerning IoT systems. To the best of our knowledge, we are the first to provide insights about those factors and decisions *in practice*.

III. Research Methodology

To conduct this study, we followed the guidelines proposed by Ciolkowski *et al.* [11]. The applied methodology comprises four phases, as presented below.

A. Phase 1 - Survey Definition

In this phase, we carried out the following activities:
(1.1) Formulate the goal of the study. We followed, for the part concerning this study, the Goal-Question-Metric approach [10], see Table I.

TABLE I
Goal of this study

Purpose	identify
Issue	the main drivers of the deployment decisions of
Object	IoT systems
Viewpoint	from the architects point of view

To *confirm the need* of the survey, we manually searched the literature for studies with similar goals. To the best of our knowledge, this paper presents the first effort that aims to achieve the goal formulated in Table I.
(1.2) Define the Research Questions (RQs). To achieve the goal of the study, we investigate the following RQs.

- *RQ1: Where are the software components of IoT systems deployed in practice?*
- *RQ2: What are the main drivers of the deployment decisions of IoT systems in practice?*

B. Phase 2 - Survey Design

In this phase, we carried out the following activities:
(2.1) Define the target population. The community of the participants consists of researchers and practitioners working on IoT systems. To build up a sample of the community, we used the following methods [17], [25]:

1) Convenience sampling: We asked our industrial partners for contacts of experts in the field of engineering IoT systems, and individually invited the suggested practitioners to participate in our survey. Additionally, we posted the link of the questionnaire in social networks (e.g., LinkedIn and Facebook).
2) Snowball sampling: We asked the practitioners nominated by our industrial partners to distribute the questionnaire in their professional networks.

To guarantee that only well-informed practitioners participate in our survey, we dropped the responses of those who declared not to have ever worked on any IoT project. One of the questions of the questionnaire refers to the professional role of the respondent, and we used its answers to identify the practitioners working as IoT architects (i.e., the subjects of interest for this study).
(2.2) Construct a conceptual model. Figure 1 presents a UML class diagram[3] that describes the main objects linked to the goal of the study and its research questions and the relations among them. Each IoT system has an *architecture* designed to meet the stakeholders' requirements. The architecture is composed of *software components*, deployed on *hardware components*. *Deployment decisions* made by architects specify the mapping between the software and hardware components. The ternary relation "Deployed Software components in Hardware components" (DSH) represents such a mapping. Multiple *Factors* can drive a deployment decision, such as the extra-functional requirements of the system and constraints like operational cost limits.

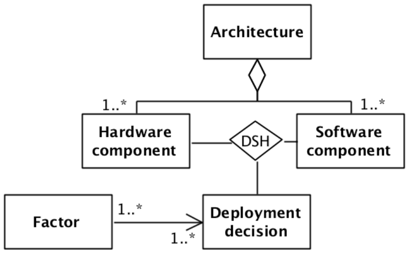

Fig. 1. Conceptual model of the study main entities

(2.3) Decide the data collection approach. As the targeted population works all over the world, we decided to collect their responses via an online questionnaire.

[2] https://www.iot-survey.com/

[3] This model comprises only the main entities related to the study, and it does not capture all the entities related to IoT systems software architectures.

(2.4) Design the questionnaire. To achieve the goal of the study and answer the formulated RQs, we consider only a small part of the questionnaire that we designed to analyze the state-of-the-practice of the Software engineering for IoT in the Industry. This part consists of questions belonging to five logical sections (a-e), designed considering the entities of the conceptual model shown in Figure 1. Note that questions in Sections b and c gave the participant indications to take into account the majority of the projects they were involved in when answering.

a. *Introduction*. In this section, we presented general information about the study, stated its goal, the targeted population, and the time needed to answer the survey.
b. *Questions about the deployment decisions*. To get insights about the deployment decisions in practice, in this section, we asked questions about the placement of the components of the IoT systems engineered by the participants considering the Edge and Cloud computing paradigms. Also, we asked questions about the leveraged protocols, the used Cloud platforms, and how satisfactory they were.
c. *Questions about the factors that drive the deployment decisions*. In this section, we asked questions about the quality attributes and constraints that drive the deployment decisions made by the participants.
d. *Personal info*. In this section, we asked in which country the participants currently work, their years of experience in the field of the IoT, their current roles, and the number of the projects and the main application domains they worked on. The answers to the questions of this section and section e below are used to draw an overview of the survey participants (see Section IV).
e. *Company info*. In this section, we asked about the companies where the participants currently work: their core business, size, number of years of activity in the field of the IoT, and IoT aspects that they focus on or provide.

The interested reader can find the questions of the overall survey questionnaire used in this study as headings of the columns in the anonymized raw data[4].

(2.5) Specify the data analysis approaches. To analyze the participant responses, we carried out the following activities.

a. *Collection of responses*. Using Google Surveys, we downloaded the practitioner answers to the questionnaire as an Excel spreadsheet where the columns correspond to the questions, and the rows to the participants.
b. *Vertical analysis*. We performed a few statistical analyses on the collected data. For closed-ended questions, we analyzed the number of occurrences of each possible answer in all the rows (i.e., vertically) [16]. For open-ended questions, we analyzed the answers and mapped them to categories. Each category has: (1) a unique identifier that replaces the answers mapped to it and is statistically analyzed afterward; (2) a textual description to specify the definition of the category [22]. For example, many countries have slightly different denominations (e.g., US, USA, or The United States), [mis]spelled in different cases. Thus, the answers to the question about the country where respondents currently work may be different though denoting the same country. We mapped (different spelling of) different names for the same country to one category (e.g., The United States) with a unique numerical identifier (e.g., 7), that replaces all the answers and is used to count the number of participants from that country. The category definition and the semantic mappings were performed by a researcher and checked by another one. We organized periodic meetings to discuss and resolve conflicts.
c. Horizontal analysis. We performed cross-tabulations to elicit possible relations among the answers of different questions [16].

(2.6) Identify threats to validity. We identified the following threats to the research validity:

a. *Sampling techniques*. Making the survey available on social media platforms can result in having fake answers, possibly by unqualified participants. To mitigate this threat, we made the survey available in selected groups that have a specific professional interest in IoT.
b. *Terminology*. Some terms can have different interpretations among researchers and practitioners. For instance, some people refer to the servers close to the Edge of the network as Fog nodes, while others consider them as Edge nodes. Therefore, such terms are clarified whenever mentioned in the questionnaire.
c. *Internal validity*. To reduce any bias that could be caused by the way we formulated the questions and the provided options for the closed-ended questions, we designed the questionnaire in an iterative approach where we asked expert researchers and architects to participate in pilot testing of the survey. We used their feedback to improve the survey and make sure that it was understandable, usable, and ready for execution. Moreover, we did not require the participants to answer all the questions, so as not to force them to select a random choice just to complete the questionnaire. Finally, we allowed free-text entries (that is, open answers), to verify the completeness of the proposed alternatives.

C. Phase 3 - Survey Implementation and Execution

To *implement the survey*, we exploited Google Surveys service[5] to create the questionnaire and make it available online. We chose this service as it enables creating and sharing questionnaires easily. It also provides a basic (graphical) analysis of the responses automatically. In the *execution phase*, we distributed the questionnaire to the targeted population and collected the responses. In this study, we present the data collected from October 2018, the survey distribution starting, to March 2019.

IV. Overview of Survey Participants

As already discussed, we used for our study a subset of the data collected in the context of a more extensive survey.

[4] http://sepl.dibris.unige.it/2020-ICSA-Survey-Deployment-IoT-Sys.php

[5] https://surveys.google.com/

Altogether, 444 people participated in the original survey, while for this study, we selected only the 66 participants with a role requiring some experience in designing architectures for IoT systems. The selected roles where “Software architect” and “Firmware architect”, among the choices proposed by the survey and other eight free-text answers, some of them expressed multiple roles like, for instance, “Firmware and Software Architect”. The other roles given by some participants were “Lead architect”, “Full-stack engineer”, and “Solution architect”. In this study, the overall set of participants consists of these 66 architects of which 81% declared to be software architects and 13% firmware architects. They work in 18 countries across the world; more specifically, in Italy (23%), India (23%), the United States (11%), Germany (9%), and smaller percentages in the following countries: Sweden, United Kingdom, Brazil, Spain, Bangladesh, Denmark, France, Iran, Ireland, Israel, Luxembourg, Poland, Tunisia, and Turkey, as shown in Figure 2.

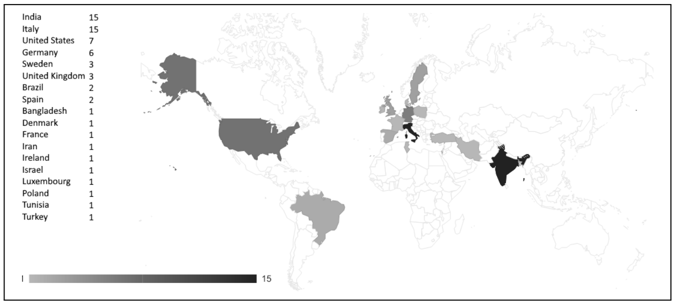

Fig. 2. Study participants working countries

The participants’ companies are representative of micro-companies counting 1-9 employees (23%), small companies counting 10-49 employees (20%), medium companies counting 50-249 employees (11%), and large companies with at least 250 employees (46%).

As shown in Figure 3, the majority of those companies do business in the software development domain, but also in several other business domains (note that a company can do business in multiple domains).

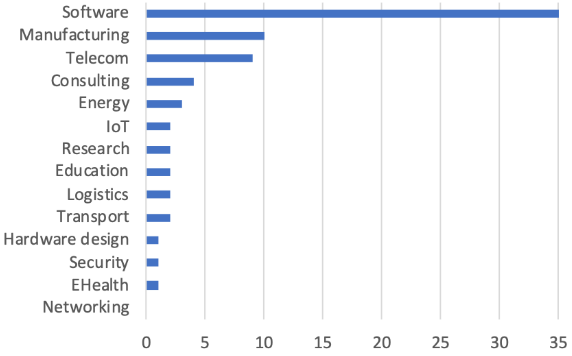

Fig. 3. Study participants companies core business

The companies focus on different aspects of IoT. The most common are IoT applications and services (83%), Sensing (60%), Communication and Computation (both 57%), Actuation (48%), and Storage (26%).

Figure 4 shows the IoT application domains of the participants’ projects. A participant could work on different projects in multiple application domains simultaneously.

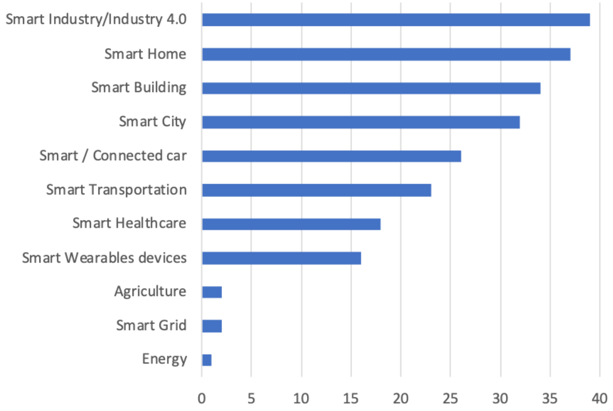

Fig. 4. Study participants projects IoT application domains

Figure 5 presents the participant experience in terms of years of practice in the field IoT. All but one respondent have worked on IoT projects for at least a year, as to be expected since the architect role requires seniority. Similarly, Figure 6 shows the participant experience in terms of numbers of IoT projects involving them. The diversities in respondents’ experience and nationality, and the many IoT application domains used in their projects guarantee the coexistence of different perspectives and contribute to the comprehensiveness of the results of the study.

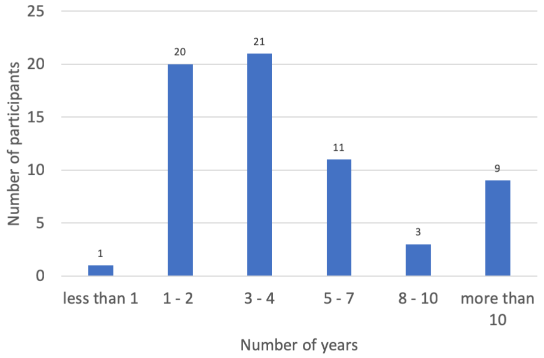

Fig. 5. Study participants years of experience in the field of IoT

V. Main Findings and Results

In this section, we report the main findings of the study that we derived by applying the data analysis approaches presented in Section III-B on the collected raw data. The main insights found are summarized below and discussed in detail in Section VI.

1) In practice, architects rely on the Cloud more than on the Edge for deploying the software components of IoT systems, in the majority of the IoT application domains.

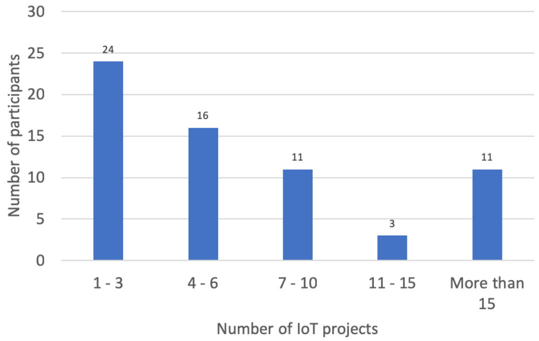

Fig. 6. Study participants IoT projects

2) The four main factors that influenced the architects' deployment decisions are reliability, performance, security, and cost.

A. *Deployment Decisions of IoT Systems*

In this section, we present the questions of the survey and the analysis of the participants' responses that we used to answer RQ1. The questions below are part of section b of the questionnaire (as described in Section III-B). In question (b.1) below, we used *computational capabilities* as a general term for software components to prevent restrictive interpretations by users of *software components* as *software adhering to some specific component model*.

Question (b.1): Where were the computational capabilities of your IoT systems deployed, in the majority of the IoT projects that you worked on ("at the Edge" means capabilities provided by IoT devices, i.e. at the Edge of the network)?

Options: Everything on the Cloud, 75% on the Cloud and 25% at the Edge, 50% on the Cloud and 50% at the Edge, 25% on the Cloud and 75% at the Edge, or Everything at the Edge.

Answers: As shown in Figure 7, the majority (39%) of the architects decided to deploy 75% of the computational capabilities of the IoT systems they engineered in the Cloud and 25% at the Edge of the network. Moreover, 23% of the architects decided to deploy the computational capabilities half in the Cloud and half in resources at the Edge.

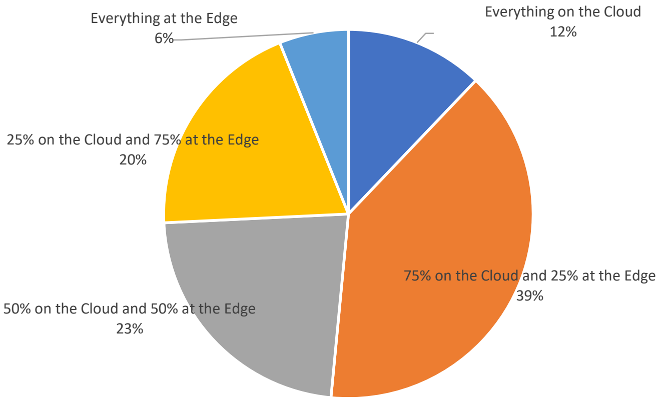

Fig. 7. IoT systems deployment decisions in the Edge-Cloud continuum

Question (b.2): Within the IoT projects that you worked on, which Cloud Platforms were used, and how satisfactory were them?

Options: Azure Sphere (Microsoft Azure IoT platform), AWS IoT Core (Amazon web services platform), Bluemix (IBM Cloud platform), In house platform, and other Cloud platforms.

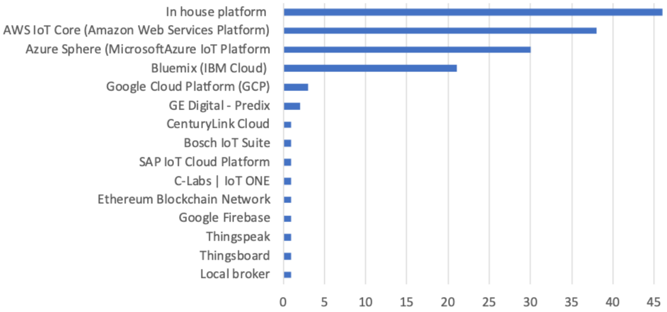

Fig. 8. The used Cloud platforms

Answers: As shown in Figure 8, the two most used Cloud platforms are in house platforms and AWS IoT Core, respectively. They were also chosen as the most satisfactory platforms, as presented in Figure 9.

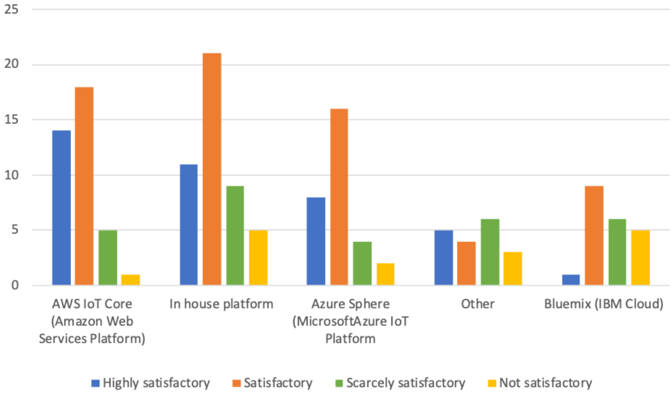

Fig. 9. Cloud platforms satisfaction level

Question (b.3): If you selected other in the previous question, which were the other used Cloud Platforms?

Answers: The architects reported the use of several other Cloud platforms, such as Google Cloud Platform and GE Digital - Predix. The complete list of the used Cloud platforms is in Figure 8.

Question (b.4): Within the IoT projects that you worked on, which protocols were used? Have you used other protocols?

Options: MQTT, CoAP, Zigbee, Bluetooth, Bluetooth Low Energy (BLE), 6LowPAN, IEEE 802 family protocols (e.g., WIFI), NFC, and/or Z-Wave.

Answers: The most used protocols were, respectively, MQTT (73%), IEEE 802 family protocols (e.g., WIFI) (67%), Bluetooth (39%), Bluetooth Low Energy (38%), Zigbee (29%), CoAP (24%), NFC (17%), 6LowPAN (15%), and/or Z-Wave (6%). Moreover, the users reported usage of other protocols but with much smaller percentages, for instance, HTTP (5%), LoRa

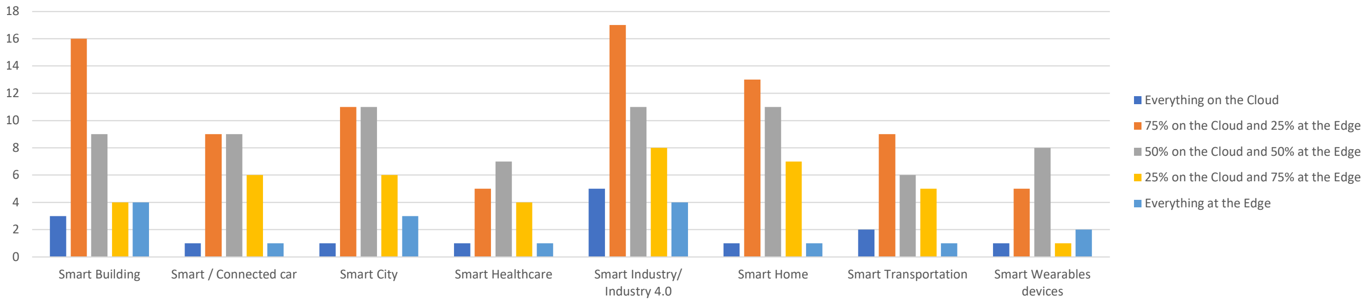

Fig. 10. IoT systems deployment decisions in different application domains

(3%), and OPC-UA (3%). Participants could select multiple protocols and possibly propose others in the free text answer; thus, the sum of the percentages may be greater than 100%.

To provide further insights, we analyzed the correlations among the deployment decisions (i.e., the answers to the question b.1) and the different application domains of the projects that the architects worked on (see Figure 4).

As presented in Figure 10, the majority of the architects expressed that in the smart buildings, Industry 4.0, smart homes, and smart transportation domains, they deployed around 75% of the software components of IoT systems in the Cloud, and 25% of the capabilities in resources at the Edge of the network. While, in the smart wearable devices and smart healthcare domains, the majority of the architects deployed the capabilities of IoT systems in resources at the Edge and the Cloud in equal percentages. Finally, in the smart cities and smart connected cars domains, the two deployment patterns *half and half in the Cloud and at the Edge* and *three quarters in the Cloud and one quarter at the Edge* are the most selected *ex aequo*.

B. Drivers of the Deployment Decisions

In this section, we present the questions of the survey and the analysis of the architects' responses that we used to answer RQ2. The questions below are part of Section c of the questionnaire (see Section III-B).

Question (c.1): Which were the main drivers for your deployment decisions, and how much were they relevant? Please, select the answers by considering the majority of your IoT projects.

Options: Size of IoT system instance, application domain/industrial vertical, security, privacy, cost, performance, and/or reliability.

Answers: Figure 11 presents how much valuable the architects deem, for deployment decisions, the different included factors, in percentage of the respondents. By assigning a symmetric linear ranking to the possible answers, with the highest value to *highly relevant*, the lowest to *not relevant*, and zero to *not applicable* so that such choices do not influence the overall score, we can rank the different factors. For instance, associating highly relevant to 2, relevant to 1, scarcely relevant to -1, not relevant to -2, and not applicable to zero, we get that architects value most reliability (90 points), performance (70), security (64), cost (58), size of IoT system (53), privacy (42), and application domain (37).

Question (c.2): Add below other drivers for your deployment decisions.

Answers: The architects reported the factors shown in Figure 12 as other drivers for their deployment decisions of IoT systems. To provide further insights, we analyzed the correlations among the deployment decisions (i.e., the answers to the question (b.1)) and the factors that drove the architects to make them (i.e., the answers to the question (c.1)).

Figure 13 presents the analysis of the participants' deployment decisions and the factors that influenced them. For each

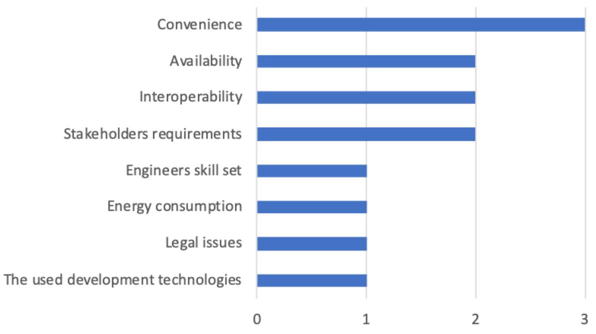

Fig. 12. Other deployment decision drivers

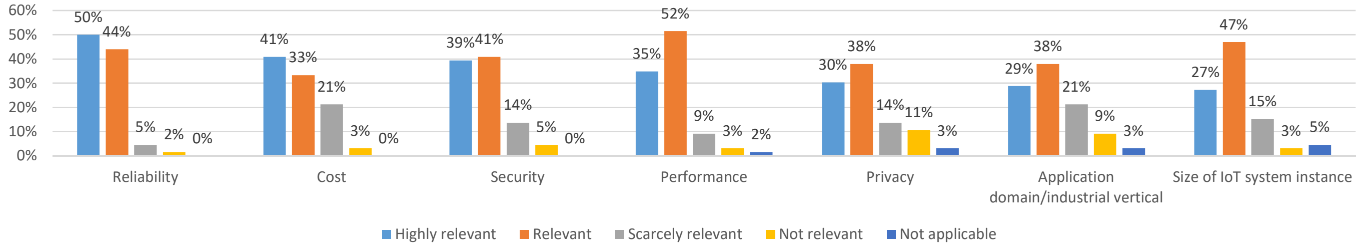

Fig. 11. Participants' deployment decisions drivers

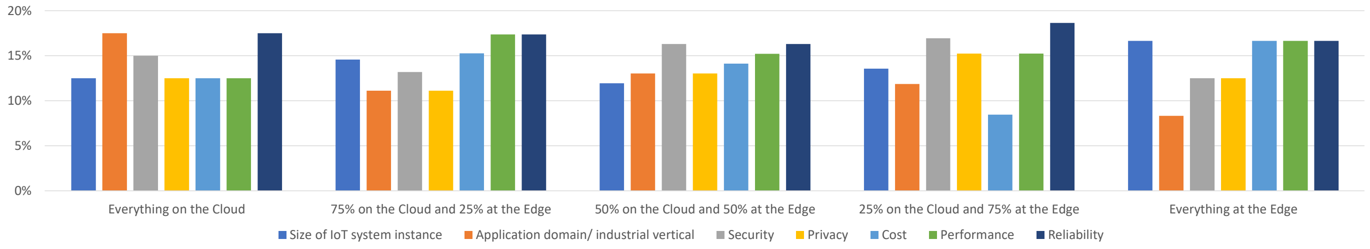

Fig. 13. Analysis of the deployment decisions and their drivers

deployment arrangement (e.g., deploying everything in the Cloud), each column in the figure shows the percentage of participants who selected a specific factor (e.g., reliability) as a deployment driver on the total number of participants who chose the same arrangement. In the most recognized category of deployment arrangements (three quarters in the Cloud and one quarter at the Edge), the deployment decisions are mainly driven by reliability and performance (around 17% each), cost and size of IoT system (around 15% each), and security (around 13%), respectively. While, in the second most recognized category of deployment decisions (half and half in the Cloud and at the Edge), security and reliability are the main drivers (around 16% each) followed by performance (around 15%), cost (around 14%), and privacy and application domain (around 13% each), respectively.

VI. Discussion

The *first finding* of the study reveals that IoT system deployment uses more commonly Cloud platforms than resources at the Edge of the network, in the majority of application domains, such as smart transportation, smart buildings, and smart industry. While architects prefer resources at the Edge of the network to deploy IoT systems in domains such as smart healthcare and smart wearable devices. Those deployment decisions were mostly driven by four main factors, which are reliability, performance, security, and cost, as expressed in the *second finding* of the study (see Section V). Another factor that might justify the preference towards Cloud platforms is that they were available for end-users before the Edge platforms.

Reliability was chosen as the most influencing factor of the deployment decisions in practice. Nowadays, assuming to have a reliable Internet connection, Cloud platforms provide a wide variety of reliable services that enable the realization of IoT systems. In contrast, in the case of unreliable Internet connections, Edge platforms would be more suitable. The AWS IoT core platform, selected as the most satisfactory platform by the architects, enables connecting billions of IoT devices and transmitting trillions of messages[6]. It runs on a global infrastructure whose service level agreement commits that the availability percentage would at least be 99.99%[7]. Additionally, when deploying systems in the Cloud, often, failures in Cloud nodes are resolved by the service providers who are also responsible for the integrity of the data stored in those nodes.

The *Performance* factor also significantly influences the deployment decisions of IoT systems in practice. Cloud infrastructures have more powerful processing capabilities than Edge infrastructures. However, they require the data to be transferred to the Cloud to be processed. Likewise, requests to the IoT devices and interactions among them should pass through the Cloud. These requirements result in high bandwidth demand and energy and latency issues that affect the quality of services of IoT systems. Edge computing addresses these issues by enabling the deployment of processes in resources close to the Edge of the network [3]. This aspect clarifies why in some application domains, such as smart connected cars, where performance is most relevant, 50% of the software components of IoT systems were deployed at the Edge.

In [2], the authors recognized *security* as the most studied quality aspect of IoT systems in the literature. The findings of the study show that security is among the factors that significantly influence the deployment decisions of IoT systems in practice. This choice can be due to several reasons, including the following ones. IoT systems can monitor sensitive data (e.g., health parameters), or control critical applications (e.g., self-driving cars) or services that can be costly (e.g., managing district heating). Thus, security aspects should be taken into consideration in all the phases of engineering IoT systems, including the deployment phase [2], [3]. When deploying the software components of IoT systems in the Cloud, the service providers are responsible for the majority of the security aspects. In contrast, when deploying the components in local resources at the Edge of the network (e.g., on-premise servers), IoT engineers are responsible for defining, performing, and monitoring all the security measures. Such a difference in the responsibility attribution might be one of the reasons for the first finding of the study.

Cost was also recognized among the most influencing factors of the deployment decisions in practice. In some cases, the high cost of using Cloud platforms could lead engineers to deploy IoT systems in resources at the Edge and the other way around (i.e., when Cloud platforms are cheap they prefer to deploy on the Cloud). The cost of deploying IoT systems in the Cloud depends on multiple factors, including the processing and storage capabilities of the requested instances and the bandwidth dedicated to exchanging the data. Some cloud platforms (e.g., AWS IoT Core) provide flexible instances that can scale automatically to meet the business needs, though often such instances cost more than the reserved ones. Some

[6] https://aws.amazon.com/iot-core/
[7] https://aws.amazon.com/compute/sla/

studies consider the cost factor when deploying IoT systems in the Edge-Cloud continuum (e.g., [9], [15]). Nevertheless, more efforts are needed to compare the different pricing models in practice.

The findings of this study reveal that *privacy*, *application domain*, and the *size of the IoT system* are also significant factors that influence the deployment decisions. In some application domains (e.g., health care or military industries), often, some data should be stored and processed in private resources at the Edge. The number and locations of the IoT devices and services that constitute IoT systems influence the deployment decisions. More specifically, Cloud infrastructures are more suitable for hosting IoT systems that are composed of large numbers of services and IoT devices scattered across wide geographical areas [3].

VII. Conclusions and Future Work

This paper presents the results of a survey on the deployment decisions concerning IoT systems in practice and the factors that influence those decisions. The survey involved 66 practitioners from 18 countries with experience in designing architectures for IoT systems in various business domains and roles.

Overall, our analysis reveals two main findings and several more detailed results associated with the survey questions. First, architects rely on the Cloud more than the Edge for deploying IoT systems. Second, the four most influencing factors that drive the architects' decisions are reliability, performance, security, and cost. To make these findings more useful to researchers and practitioners, we plan to investigate the trade-offs among the factors and identify concrete evaluation metrics for each of them. Additionally, we plan to interview expert IoT practitioners to gain deeper insights and provide recommendations about how to design optimal deployment models for IoT systems. Moreover, our current work on analyzing the other data collected by the complete survey with 444 participants aims at investigating the State-of-the-practice of the Software Engineering for IoT in the Industry. The survey will provide insights into several aspects, including the characteristics of IoT systems and their development life cycle.

Acknowledgment

This work is partially financed by the Knowledge Foundation through the Internet of Things and People research profile (Malmö University, Sweden).

References

[1] Akbar, M. A. and Kamal, T. and Baddour, A. M. Identification of Privacy and Security Risks of Internet of Things: An Empirical Investigation. *Review of Computer Engineering Research*, 2019.

[2] Alkhabbas, F. and Spalazzese, R. and Davidsson, P. Characterizing Internet of Things Systems through Taxonomies: A Systematic Mapping Study. *Internet of Things*, 7:100084, 2019.

[3] Ashouri, M. and Davidsson, P. and Spalazzese, R. Cloud, Edge, or Both? Towards Decision Support for Designing IoT Applications. In *2018 Fifth International Conference on Internet of Things: Systems, Management and Security*, pages 155–162. IEEE, 2018.

[4] Ashouri, M. and Lorig, F. and Davidsson, P. and Spalazzese, R. Edge Computing Simulators for IoT System Design: An Analysis of Qualities and Metrics. *Future Internet*, 11(11):235, 2019.

[5] Atzori, L. and Iera, A. and Morabito, G. The Internet of Things: A Survey. *Computer networks*, 54(15):2787–2805, 2010.

[6] Brogi, A. and Forti, S. QoS-aware Deployment of IoT Applications through the Fog. *IEEE Internet of Things*, 4(5):1185–1192, 2017.

[7] Brogi, A. and Forti, S. and Guerrero, C. and Lera, I. How to Place Your Apps in the Fog-State of the Art and Open Challenges. *arXiv preprint arXiv:1901.05717*, 2019.

[8] Brogi, A. and Forti, S. and Ibrahim, A. How to Best Deploy your Fog Applications, Probably. In *2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC)*, pages 105–114. IEEE, 2017.

[9] Brogi, A. and Forti, S. and Ibrahim, A. Deploying Fog Applications: How Much Does it Cost, by the Way? In *CLOSER*, pages 68–77, 2018.

[10] Caldiera, V. R. B. G. and Rombach, H. D. The Goal Question Metric Approach. *Encyclopedia of Software Engineering*, pages 528–532, 1994.

[11] Ciolkowski, M. and Laitenberger, O. and Vegas, S. and Biffl, S. Practical experiences in the design and conduct of surveys in empirical software engineering. In *Empirical Methods and Studies in Software Engineering*, pages 104–128. Springer, 2003.

[12] Guan, X. and Wan, X. and Choi, B. and Song, S. and Zhu, J. Application oriented dynamic resource allocation for data centers using docker containers. *IEEE Communications Letters*, 21(3):504–507, 2016.

[13] Guerrero, C. and Lera, I. and Juiz, C. A lightweight decentralized service placement policy for performance optimization in fog computing. *J. of Ambient Intelligence and Humanized Computing*, 10(6):2435–2452, 2019.

[14] Gupta, H. and V. D., Amir and Ghosh, S. K. and Buyya, R. iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. *Software: Practice and Experience*, 47(9):1275–1296, 2017.

[15] Hassan, M. A and Xiao, M. and Wei, Q. and Chen, S. Help Your Mobile Applications with Fog Computing. In *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking-Workshops (SECON Workshops)*, pages 1–6. IEEE, 2015.

[16] Kasunic, M. Designing an Effective Survey. Technical report, Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2005.

[17] Kitchenham, B. and Pfleeger, S. L. Principles of survey research: part 5: populations and samples. *ACM SIGSOFT Software Engineering Notes*, 27(5):17–20, 2002.

[18] Kowatsch, T. and Maass, W. IoT-I Deliverable - D2.4: Social Acceptance and Impact Evaluation. Work report, IoT-I consortium, 2012.

[19] Kruchten, P. B. The 4+ 1 view model of architecture. *IEEE software*, 12(6):42–50, 1995.

[20] Leotta, M. and Ricca, F. and Ribaudo, M. and Reggio, G. and Astesiano, E. and Vernazza, T. An Exploratory Survey on SOA Knowledge, Adoption and Trend in the Italian Industry. In *Proceedings of 14th International Symposium on Web Systems Evolution (WSE 2012)*, pages 21–30. IEEE, 2012.

[21] Mahmud, R. and Kotagiri, R. and Buyya, R. Fog computing: A taxonomy, survey and future directions. In *Internet of Everything*, pages 103–130. Springer, 2018.

[22] Miles, M. B. and Huberman, A. M. *Qualitative data analysis: An expanded sourcebook*. sage, 1994.

[23] Miorandi, D. and Sicari, S. and De Pellegrini, F. and Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad hoc networks*, 10(7):1497–1516, 2012.

[24] Nguyen, P. and Ferry, N. and Erdogan, G. and Song, H. and Lavirotte, S. and Tigli, J. and Solberg, A. Advances in Deployment and Orchestration Approaches for IoT-a systematic review. In *2019 IEEE International Congress on Internet of Things (ICIOT)*, pages 53–60. IEEE, 2019.

[25] Patton, M. Q. *Qualitative Evaluation and Research Methods*. SAGE Publications, inc, 1990.

[26] Reggio, G. and Leotta, M. and Ricca, F. Who knows/uses what of the UML: A personal opinion survey. In *Proceedings of 17th International Conference on Model Driven Engineering Languages and Systems (MODELS 2014)*, volume 8767 of *LNCS*, pages 149–165. Springer, 2014.

[27] Shi, H. and Chen, N. and Deters, R. Combining mobile and Fog Computing: Using CoAP to link mobile device clouds with Fog Computing. In *2015 IEEE International Conference on Data Science and Data Intensive Systems*, pages 564–571. IEEE, 2015.