Crowd-Driven IoT/IoE Ecosystems: A Multidimensional Approach

Xenia Ziouvelou, Panagiotis Alexandrou, Constantinos Marios Angelopoulos, Orestis Evangelatos, Joao Fernandes, Nikos Loumis, Frank McGroarty, Sotiris Nikoletseas, Aleksandra Rankov, Theofanis Raptis, Anna Ståhlbröst and Sebastien Ziegler

Abstract During the past few years an astonishing paradigm shift has occurred towards a new participatory value creation model driven by users. Open collaborative innovation practices have emerged in which an increasing number of users mutually collaborate by openly communicating their ideas, sharing best practices, and creating new knowledge across sectors. These online, distributed, crowd-driven networks take advantage of underlying network effects in order to harness the collective power and intelligence of the Crowd. Such novel paradigms fuel an

X. Ziouvelou (✉) · F. McGroarty
University of Southampton, Southampton, UK
e-mail: p.ziouvelou@soton.ac.uk

F. McGroarty
e-mail: f.j.mcgroarty@soton.ac.uk

P. Alexandrou · S. Nikoletseas · T. Raptis
Computer Technology Institute & Press Diophantus, Patras, Greece
e-mail: aleksandro@ceid.upatras.gr

S. Nikoletseas
e-mail: nikole@cti.gr

T. Raptis
e-mail: traptis@ceid.upatras.gr

C.M. Angelopoulos · O. Evangelatos
Université de Genève, Geneva, Switzerland
e-mail: Marios.Angelopoulos@unige.ch

O. Evangelatos
e-mail: orestis.evangelatos@unige.ch

J. Fernandes
Alexandra Instituttet A/S, Aarhus, Denmark
e-mail: joao.fernandes@alexandra.dk

N. Loumis
University of Surrey, Guildford, UK
e-mail: nikolaos.loumis@surrey.ac.uk

J.M. Batalla et al. (eds.), *Beyond the Internet of Things*,
Internet of Things, DOI 10.1007/978-3-319-50758-3_14

increasing interest in mobile crowdsensing (MCS) methods in the context of IoT/IoE, which leverage the power and the wisdom of the crowd to observe, measure, and make sense of particular phenomena by exploiting user-owned mobile and wearable devices. However, when one examines the design and development of such ecosystems, realises that there is a gap in existing research. While emphasis has been placed upon the technical aspects, the success of such ecosystems is dependent on a number of diverse criteria. This chapter aims to fill this gap by providing a framework, which adopts a holistic approach based on multiple perspectives (namely technical, business, and people perspectives) and facilitates the design and development of crowd-driven ecosystems. This model is examined in the context of a hybrid crowd-driven IoT/IoE ecosystem, IoT Lab, in order to exemplify how these perspectives can be used to promote an ecosystem's success and detail the challenges faced. This analysis is extended through the introduction of the "*Crowd-driven Ecosystem Index (CEI)*", which measures the coverage intensity of each of the key ecosystem parameters, denoting this way the propensity of success of a crowd-driven network.

1 Introduction

We are witnessing an ever-increasing interest in actively engaging with the crowd for particular purposes that range from simple ratings to task-oriented activities, and from problem solving to innovation creation across different industrial sectors. A paradigm shift has occurred towards a new participatory value creation model driven by users. As such, open collaborative value creation ecosystems have emerged providing an environment that nurtures this change in the role of the users from passive to active co-creators. These online, distributed crowd-driven networks leverage the network effects so as to harness the collective power and intelligence. Within these ecosystems users actively collaborate by openly communicating their ideas and data, sharing best practices and creating new knowledge that augments our innovation potential across various sectors.

As a result, recently there has been an increasing interest in studying the integration and the corresponding potential of this emerging participatory model in the

A. Rankov
DunavNET, Novi Sad, Serbia
e-mail: aleksandra.rankov@dunavnet.eu

A. Ståhlbröst
Luleå University of Technology, Luleå, Sweden
e-mail: anna.stahlbrost@ltu.se

S. Ziegler
Mandat International, Geneva, Switzerland
e-mail: sziegler@mandint.org

context of the Internet of Things (IoT)/Internet of Everything (IoE)[1] paradigm. This interest has also been fuelled by the high acceptance rates of truly portable hand-held and wearable smart devices that enable the creation of crowd-driven networks. These networks seek to exploit the embedded sensing capabilities and the intrinsic mobile nature of such devices. Consequently, the IoT/IoE environment has introduced new user-centric sensing paradigms, like mobile crowd sensing (MCS) [3, 4], that go beyond traditional sensing techniques (e.g., sensor networks, etc.,) by leveraging both the power and the wisdom of the crowd. These paradigms enable the IoT/IoE environment to sense, observe, measure, and make sense of real-world conditions (e.g., environmental, etc.,) and activities (e.g., personal activities and interactions, etc.,) by engaging user-owned mobile and wearable devices.

However, despite the promising participatory value creation paradigm and the numerous advantages that it provides, crowd-driven IoT/IoE ecosystems are still in their initial stages and facie many challenges as their success relies on several crucial elements. Due to their nature, these ecosystems necessitate that multi-disciplinary perspectives are addressed and combined during their conception and development processes. The fact that these networks are driven both by the research community and several organisations, makes it even more challenging to integrate and drive an optimal solution. As an example, motivators and support for incentives must be investigated in different perspectives, namely business, technology and end-user (people) perspectives, in order to understand for each one of them what are the corresponding needs, barriers, constraints, etc. and therefore conceptualise a model that addresses them in a combined way. Such a model will facilitate towards this end both the design and the development of successful crowd-driven ecosystems.

To the best of our knowledge, existing research efforts place emphasis only upon the technical aspects of the design and development of crowd-driven ecosystems. On the contrary, little attention is put on how this process should be designed and undertaken accounting for non-technical ecosystem elements as well. This chapter identifies and addresses this gap by providing a framework, which adopts a holistic approach based on multiple perspectives (technical, business and people perspectives) and facilitates the design and development of crowd-driven ecosystems.

This chapter is organised as follows: Sect. 2 presents the evolution of ecosystems placing emphasis on the emerging crowd-driven ecosystems and presents a taxonomy of the key aspects of each type of ecosystem. Section 3 presents a multi-dimensional approach for the design and development of crowd-driven ecosystems. While, Sect. 4 examines the proposed model in the context of a hybrid crowd-driven IoT ecosystem, namely IoT Lab, and introduces the "*Crowd-driven*

[1]Due to the non-existence of a standard IoT definition [1] one can identify a variety of IoT definitions in the existing literature. The spectrum includes both narrow definitions, which perceive IoT only as an interconnection of "things" and broad ones that view the IoT idea as implying concepts that relate to the interconnection of people, processes and data in addition to "things" [2]. As such, in the course of this chapter we perceive IoT and IoE as acronyms for the same conceptual paradigm.

Ecosystem Index (CEI)", which measures the coverage intensity of each of the key ecosystem parameters, denoting this way the propensity of success of a crowd-driven network. The chapter concludes in Sect. 5.

2 The Rise of Crowd-Driven Ecosystems

The notion of ecosystems is directly linked to the natural world. Coined in 1935 by the British botanist Arthur Tansley [5], the notion of ecosystems was introduced in order to denote a community of living organisms interacting with each other and their environment as a system. Such ***biological ecosystems*** were considered to be evolving systems, that are "dynamic, constantly remaking themselves, reacting to natural disturbances and to the competition among and between species" [6], p. 11. As an analogue of such biological ecosystems, the concept of ***industrial ecosystems*** was presented a few years later [7] denoting ecosystems where all material is recycled infinitely and efficiently by changing the habits of manufacturers and consumers maintaining this way our standard of living without causing environmental devastation [7], p. 145. In the business context it was Moore [8] [2] who made the parallel and proposed that a company can be viewed "not as a member of a single industry but as part of a business ecosystem that crosses a variety of industries" (p. 76). This transition from standalone companies to integrated corporate systems and eventually crowd-driven ecosystems is powered by technology, user participation and the move towards open innovation [10]. Emerging crowd-driven ecosystems leverage the network effects and harness the collective intelligence of a large number of contributors. Four distinct ecosystem types are distinguished in this chapter: knowledge ecosystems, business ecosystems, innovation ecosystems and crowd-driven ecosystems. In the sections that follow, we provide a short overview of these ecosystem concepts and provide a taxonomy (Table 1).

Existing business literature has long recognised the advantages of geographically clustered organisational entities that benefit from their co-location and the dynamic knowledge interactions that occur between them [11]. Such ***knowledge ecosystems*** play a central role in increasing knowledge creation and the speed of innovation diffusion [12] through evolutionary networks of collaboration [13]. In the online environment, such knowledge interactions can be identified within open source communities where knowledge creation and co-creation among community members that exhibit virtual proximity/co-location [14] is evident. Although research in knowledge ecosystems has implicitly assumed that such knowledge ecosystems evolve into business ecosystems, existing studies in the area indicate that there is a

[2] According to Moore, a business ecosystem is "an economic community supported by a foundation of interacting organizations and individuals—the organisms of the business world" [9]. As he suggests it is "conscious choice" that differentiates between ecological and social systems [9], p. 18.

Table 1 Taxonomy of the different types of ecosystems

	Knowledge ecosystem	Business ecosystem	Innovation ecosystem	Crowd-driven ecosystem
Function	New knowledge creation	Customer value (knowledge commercialisation)	Innovation creation/co-innovation	Crowd-driven shared value creation/co-creation
Connectivity	Decentralised and distributed	Geographically clustered or Global and distributed	Geographically clustered or Global and distributed	Global and distributed
Mode	Physical or online	Physical or online	Physical or online	Online
Relationships	Synergetic and co-operative	Competitive and collaborative ("co-opetion")	Co-operative, collaborative	Co-operative and collaborative (mass collaboration)
Openness	High degree of openness or closed	Various degrees of openness	High degree of openness or closed	High degree of openness
Structure	Dynamic inter-organisational, inter-personal	Dynamic or static, and inter-organisational	Dynamic inter-organisational and inter-personal	Dynamic
Key actor	University, research organisation/institute	Large company	Large company or community	NGO/Non-profit initiative or community or company

(Own elaboration extending [15, 17])

disconnection between the development of each type of ecosystem as the have different value creation processes [15]. ***Business ecosystems*** are seen as economic communities of interacting "organisms of the business world" [9], p. 9 with many horizontal relations with a "coopetition" structure (both collaborative and competitive relationships) [8] aiming to jointly deliver a product or service to customers [15]. According to Moore, such ecosystems are a composition of customers, lead producers, competitors, and other stakeholders,[3] while "the keystone species", are leadership companies with a strong influence [9], p. 25. Business ecosystems focus on the commercialisation of knowledge and aim to deliver value to the end users as an interrelated system of interdependent companies rather than as individual companies ([15, 17]). These nested business networks act as a source of competitive advantage for individual business entities, and depending on the ecosystems' degree of productivity, robustness and ability to create opportunities for new firms the can succeed [18]. The online environment facilitates the creation, co-evolution and expansion of such ecosystems across diverse business sectors.

Innovation ecosystems, on the other hand, can be either physical or online/virtual networks that focus on fostering creativity, as well as, triggering, developing and diffusing innovation and enabling technological development among diverse entities in an open or closed context. They are based on successful examples of agglomeration whether in geographic, economic, industrial or entrepreneurial terms [19] and unlike business ecosystems, they lack the customer (demand) side [20]. Innovation ecosystems have emerged as a multilevel, multimodal, multinodal, and multiagent system of systems [21] where innovation, co-creation, and co-innovation occur in order to generate shared value [22]. Living labs are seen as open innovation ecosystems centered on systematic user co-creation practices, which integrate research, and innovation practices in real life communities and settings.

The emergence of ***crowd-driven ecosystems***, has been powered by technology, open innovation, and participatory value creation processes driven by users. These virtual distributed ecosystems have created a global meta-environment for facilitating a change in the role of the users from passive to active creators, co-creators, collaborators and co-innovators. Crowd-driven ecosystems leverage the distributed network effects and harness the collective power and intelligence of the user community that massively collaborates [23] creating in such a way shared value [24]. These open, collaborative user-driven, value creation ecosystems enable individuals to collaborate by openly communicating their ideas, sharing data, best practices and creating new knowledge that enhances the innovation potential of our society. In particular, they explore the direct and indirect interactions with the user community through crowdsourcing, crowdsensing and crowdfunding processes harnessing this way the collective crowd capital.

This ability to exploit the capacity of the crowd has been fueled by the Internet of Things (IoT)/Internet of Everything (IoE), introducing new user-centric

[3]See [16] for an overview of business ecosystems and literature in relation to peripheral and non-peripheral actors in the business ecosystem definition.

paradigms, such as mobile crowd sensing (MCS) [3, 4]. MCS goes beyond traditional sensing techniques (e.g., sensor networks, etc.,) leveraging both the power and the wisdom of the crowd in order to sense, observe, measure and make sense of real-world conditions (e.g., environmental, etc.,) and activities (e.g., personal activities and interactions, etc.,) using user-owned mobile and wearable devices. ***Crowd-driven IoT/IoE ecosystems*** can exist in many forms, concentrating on specific crowd-driven functions (crowdsourcing, crowdsensing, crowdfunding, etc.,) or, increasingly, they can be hybrid; not tied to a specific mode. In the former case, we can identify mobile crowdsourcing ecosystems such as OpenStreetMap (crowdsourced map of the world), Waze (crowd-driven traffic navigation) as well as, web-based ones such as Amazon Mechanical Turk. Similarly, in the context of crowdsensing ecosystems we can identify networks such as PhoneLab (open access smartphone testbed), Ushahidi (user geo-location data) and APISENSE (crowd-sensing for experimental datasets) among others that monitor from city noise [25], to climate [26] and emergencies [27].

One can identify only a few crowd-driven ecosystems that integrate both crowdsourcing and crowdsensing perspectives. Examples of such distributed hybrid crowd-driven IoT/IoE ecosystems are *mCrowd* (crowdsourcing and participatory sensing) and *EpiCollect* (crowdsourcing and crowdsensing for survey purposes), which cover crowdsourcing and crowdsensing elements just partially. Additionally, they do not facilitate the integration of existing physical IoT testbeds and existing FIRE testbeds with any crowd-driven resources such as smartphones. To our knowledge, the only crowd-driven IoT ecosystem that integrates both crowdsourcing and crowdsensing (opportunistic and participatory sensing) elements, while it assimilates smartphones with existing testbeds, is *IoT Lab*.

However, when one examines the design and development of such crowd-driven ecosystems, would find a gap in existing research. To date the emphasis is placed only on technical perspectives related to crowd-driven IoT/IoE ecosystems. While the existing literature gives a lot of emphasis upon the technical aspects for the development of such networks and provides useful insights into what needs to be addressed; there is relatively little direction on how this process should be designed and undertaken, accounting for non-technical ecosystem elements. Hence, there is a need for a unified framework that embraces a holistic approach, to address different parameters that are of critical importance for the design and development of such crowd-driven ecosystems is required.

3 Crowd-Driven Ecosystems: A Multidimensional Approach

Our examination of the various crowd-driven ecosystems enables us to identify key perspectives that describe them and facilitate a holistic analysis as well as a set of key thematic areas that detail further such ecosystems (Fig. 1). The first is the people-centric perspective that encompasses the crowd views and needs for the

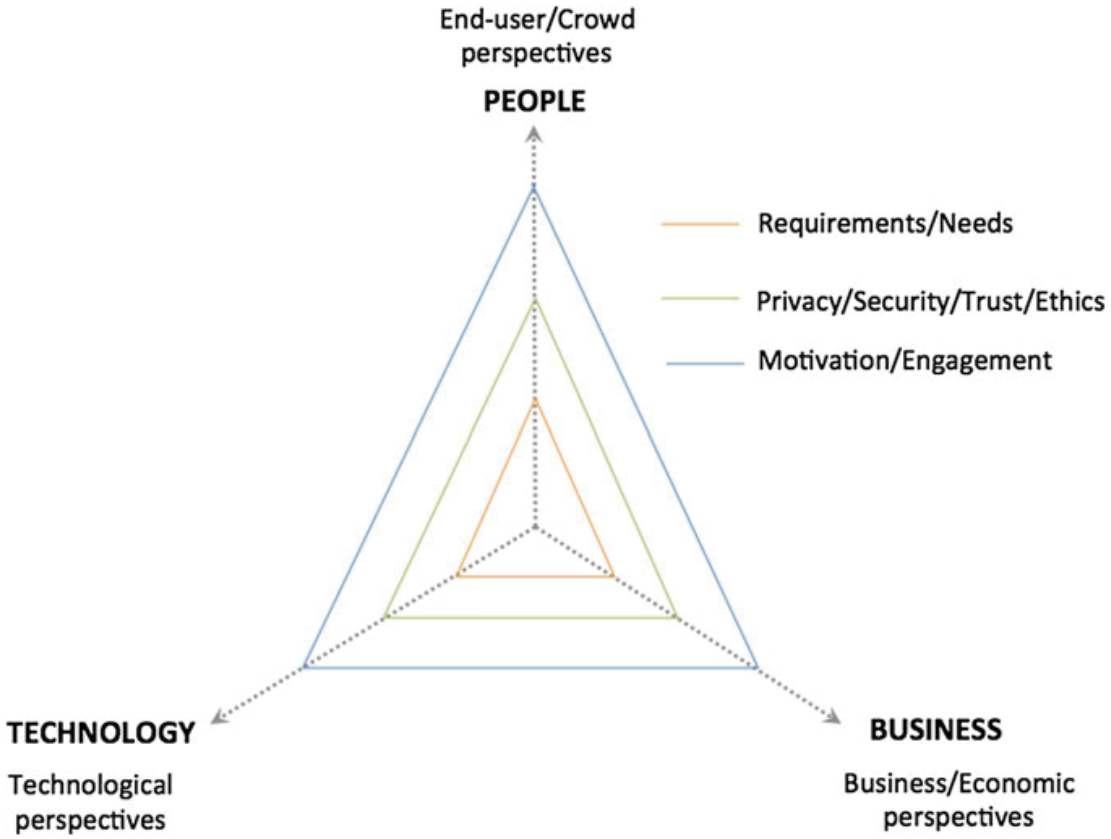

Fig. 1 A multi-dimensional model for crowd-driven IoT/IoE ecosystems

creation and co-creation of value within a given network. These needs are centered on both direct (e.g., privacy, security, trust, etc.) and indirect requirements (e.g., motivation, engagement, ethics, etc.). Secondly, the business-centric perspective whose focus is the generation of economic and business value of a given crowd-driven ecosystems; factors that affect the network sustainability. Lastly, the technology-centric perspective focuses on the technological aspects (e.g., ecosystem architecture and components, technological resources, etc.) relevant to the design and development of a crowd-driven network. The above aspects connect the people-and business-centric perspectives while integrating emerging technological advancements.

In order to further analyse these perspectives we identified some key horizontal thematic areas which describe each of these perspectives and involve: (a) *requirements and needs*: entails the definition of the needs and conditions to be fulfilled as well as the assessment of the relative importance or "value" of these specifications; (b) *privacy, security, trust and ethics*: involves the identification of each of these elements in the context of a given crowd-driven ecosystem and exploration of the inter-relationship between them, aiming to align them so as to ensure the success of the ecosystem; and (c) *motivation and engagement*: consists of overcoming the obstacles of adoption by achieving and sustaining high levels of user participation and active involvement throughout the life-cycle of the ecosystem. The sections that

Table 2 Parameters to be considered for the design and development of crowd-driven IoT/IoE ecosystems

Key thematic areas	Perspectives		
	Technical perspective	Business perspective	People perspective
Requirements/Needs	• Components of the system/types • Interactions between the components/networking • Types of Resources and their representation • Services provided/supported • Technologies invoked/used • Scalability/Resilience/Modularity • Organisation/platform – future extensions • External factors/threats to the system/access control • Interaction with end-users • Heterogeneity of data collected from the crowd • QoS (Quality of Service)	• Ecosystem structure and governance • Ecosystem business model (value creation and value capture) • Value creation: – Identify a unique value proposition (unique product/service/offering that provides value for each stakeholder of the ecosystem) – Value co-creation – Value creation for the partner/collaborator network • Value capture • Sustaining the crowd-driven networked ecosystem: Identify sustainability model (economic, community and innovation perspectives of sustainability) & co-evolution model	• Stimulate users' needs of the system, and their needs in the system • Engaging and interesting cases • Easy to use • Intuitive and encouraging design • Measurement of the crowd activity/quality of the crowd involvement/Crowd preferences • Users in control • Status of ongoing activities • User achievements visibility
Privacy/Security/Trust/Ethics	• Privacy/security/integrity/trust • Privacy by design approach • Personal data protection norms • Identity management • Information Security • Data/information integrity • Perceived trustworthiness of the system • Clear description of the required data to the user (provided by either user or device)	• Ensure security and privacy of the system and convey to crowd and ecosystem stakeholders • Clarify data ownership and privacy • Facilitate the creation of secure and trusted relationships on top of the technical secure/privacy-aware/trusted infrastructure • Ensure ethical ecosystem practices • Internal business reputation mechanisms	• Clear description of the required data (provided by either user or device) needed • Secure, trusted and easy to use system • Personal integrity intact throughout the use • Design for the right to be forgotten • Crowdsensing:

(continued)

Table 2 (continued)

Key thematic areas	Perspectives		
	Technical perspective	Business perspective	People perspective
	• Relation between the trustworthiness and privacy concerns • Transparency in information security important for trustworthiness of the system and participation rate • DB protection from external attacks • Reputation		• Opportunistic sensing (coming from people) and information security – Data from sensors is involuntary – No control over data collection (what, when, where) – Raises serious privacy concerns – Design for the right to be forgotten • Crowdsourcing • Participatory crowdsourcing – Voluntary data gathering method – individual chooses what she/he wants to report to the system – Minimal privacy concerns but no control after reporting – Important information security, integrity, availability to correct stakeholders

(continued)

Table 2 (continued)

Key thematic areas	Perspectives		
	Technical perspective	Business perspective	People perspective
Motivation/Engagement	• End-user involvement from conception to product • Importance of co-design and co-creation for defining the technical product • Understanding the crowd needs • Consideration of requirements from multi-stakeholder perspective • Paying/incentives • Incentive mechanisms	• Motivate and engage with the crowd and all different ecosystem stakeholders: incentive mechanisms design • Address ecosystem evolution parameters and crowd motivation and engagement	• Understanding what motivates the crowd and their participation • Fun • Fame • Fortune • Fulfilment

follow describe in detail the different perspectives. An overview of the key factors for each perspective is presented in Table 2 so as to facilitate the design and development of crowd-driven IoT and IoE ecosystems.

(a) ***People's Perspective***

Viewing the crowd-driven eco-system from a people's perspective set emphasis on understanding what triggers people to start using the system and what keeps them continue participating in it. At this point, it is important to understand the *needs and requirements* of the end-users, in order to ensure that they get a value from using the system. We must underline the fact that users' needs should be satisfied on two different levels focusing both on the needs of the system and needs in the system. More specifically, a crowd driven eco-system should offer a high level of attractiveness, usability, and foster engagement in the crowd. Usually, in crowd-driven eco-systems, the crowd is consisted by end-users who participate on their spare-time without any previous training, or by being forced or paid to use the system. Consequently, a crowd-driven platform must be very easy to use with a low entrance barrier that creates a clear value for the end-users.

To ensure that end-users wants to participate in, and contribute to, crowd-driven ecosystem it is also important that they can feel safe and secure and that their privacy maintains intact privacy even if they share personal data. This means that end-users privacy must be protected on two different levels, one being the data protection and how the personal data (e.g. personal profile) is protected, managed, used and stored in the back-end systems and the other level being the user interface of the intermediary platform where privacy is related to what is shown about the crowd participants in a public sphere in the platform, i.e. user profiles, engagement in tasks, data they have shared, i.e. the system must be transparent and open. Today data is increasingly viewed as the "holy grail" to understanding end-users and to foster innovation. In many crowd-driven eco-systems end-users share some of their data consciously and openly, such as personal profiles and e.g. photos, but end-users can also share data that is not as obvious and aware to them such through their smart phones sensors, or other wearables, i.e. participatory sensing. Hence, these types of systems should follow privacy-by-design principles that make the users safe and not having to consider all possible threats that they might face from using the system. Hence, individuals should have the power to determine when, how and to what extent information about them is communicated to others [28, 29].

While ensuring that end-user privacy is protected by the crowd-driven ecosystem, equally important is to understand what *motivate* the crowd to achieve the best outcome of crowdsourcing [30] and crowdsensing. In previous research on crowdsourcing and motivation (e.g., [31–33]), factors such as enjoyment, career concerns, satisfying intellectual interest, increase of status, supporting the community, feeling affiliated and create social contacts have been identified. Research has led to the conclusion that crowds are motivated differently depending on the type of crowdsourcing initiative they are engaged in [34]. For instance, in collaborative crowdsourcing such as Zooniverse and OpenIdeo, contributing to a larger

cause is what mainly motivates the crowd. While in compensation focused crowdsourcing, such as Amazon Mechanical Turk and iStockPhoto, the crowd is mainly motivated by the possibility to earn money and in competition focused crowdsourcing, such as InnoCentive and NineSigma, the main motivator is the challenge and to win a prize. Overall, motives such as enjoyment, having fun and the ability to kill time with meaningful activities, stretches along all different types of crowds. Hence, motivations for crowds can be summarised into fun, fame, fortune and fulfilment.

(b) ***Technical Perspective***

From a technical perspective, crowd-driven ecosystems require a focus on the technological enablers needed for leveraging crowdsourced infrastructure as experimental resources and potentially federating them with other IoT experimenting facilities. With respect to "*requirements and user utility*", a virtualisation roadmap of crowdsourced resources is needed. In order for the devised solutions to be replicable, the roadmap should employ standardised federation and virtualisation architectures such as the Slice Based Federation Architecture (SFA); the de facto standard used nowadays for experimental resources virtualisation and federation. Up until now, SFA has been used for federating resources of computer networks. Therefore, in order to also effectively address emerging paradigms, such as Mobile Crowdsensing Systems, SFA needs to be significantly extended appropriately so as to also include crowdsourced and other IoT resources. One potential extension of the representation and abstraction mechanisms could take place via the IPSO Application Framework that defines the communication interfaces of constrained embedded devices and smart objects that would enable crowdsourced resources to be represented as regular IoT resources. A second necessary extension is the design and implementation of such mechanisms that support the opportunistic integration of crowdsourced resources (e.g. smartphones, tablets, etc.) with the corresponding Mobile Crowdsensing functionalities. Such an extension would empower experimenters to opportunistically augment the capabilities of experimental facilities and establish two-way interaction schemes with the end-users (e.g. push notifications and reception of sensory readings and user feedback). Crowd-driven ecosystems, due to the strong personal nature of corresponding devices (e.g. smartphones) raise significant issues that are not present in regular IoT resources. In order to properly address this sensitive nature of personal devices, several privacy, anonymity and security mechanisms need to be integrated, in order to offer an increased level of trustworthiness towards the end-users providing access to their personal devices. In this respect, the integration of crowdsourced resources that can be provided by the general public raises important challenges with respect to "*Privacy, security, trust and ethics*". In order to efficiently and effectively address such issues technical solutions guaranteeing privacy and anonymity for the contributors need to be considered as well as multi-dimensional authentication and authorisation methods that enable the collected data to be treated in a secure way; for instance, to guarantee security when transmitting, storing and accessing data.

With respect to "*motivation and engagement*", technical perspectives may focus both on the users of a platform and to the crowd contributing to a crowdsourced facility. The users of crowd-driven platforms in most cases consist of researchers who seek to exploit the diverse and numerous resources available. Therefore, such a platform needs to take under consideration technical solutions that guarantee scalability, resilience, and efficiency. For instance, in order to provide an efficient way of representing all the available resources, while being able to store vast volumes of data,, hybrid database schemes shall be considered, as they combine both relational and non-relational databases. The contributors of the platform—which is the general public—can be provided with a crowdsourcing tool, e.g. a smartphone application, with an appealing and modern "look and feel" that will be non-intrusive to the smartphone user.

(c) ***Business Perspective***

The business perspective places emphasis upon the economic activity related to the crowd-driven ecosystem. As such, it examines the value creation and capture, processes within similar ecosystems, as well as, the creators and co-creators of the aforementioned value. This perspective is centered on three generic thematic areas, presented above, as it can be seen in Table 2. Concerning "*requirements and needs*", the main attention of the business perspective is paid to the ecosystem structure and governance and its business model of the key value creation and value capture elements. When it comes to the ecosystem value creation, it is critical to identify the unique value proposition of the ecosystem, in order to provide value and increase the utility of all the different ecosystem entities, as well as, to explore the value co-creation processes and its co-creators. Another essential parameter of the crowd-driven ecosystem relates to its sustainability. As such, the identification of the appropriate sustainability model is critical so as to analyse different sustainability variables such as economic, community and innovation perspectives, in addition to the evolution of the crowd-driven network itself and how this impacts its sustainability.

"*Privacy, security, trust and ethics*", constitutes a central thematic area for the business perspective as it significantly impacts the ecosystem adoption. As such, it focuses upon initially ensuring the security and privacy of the crowd-driven ecosystem and subsequently conveying this assurance to the crowd and all ecosystem stakeholders via appropriate set of policies and rules of conduct, while also defining data ownership principles within the ecosystem. These elements will set the basis for the creation of secure and trusted relationships as an additional layer above a technically secure (system security and data security within the ecosystem), privacy-aware and trusted infrastructure. In addition, the business perspective also examines the design of intra-ecosystem reputation mechanism(s), creating this way reputation capital for the ecosystem users and its activities, which will enhance further the creation of trusted environment. Given the role of ethics in the formation of trust, the adoption of ethical practices (code of ethics) within a

crowd-driven ecosystem is critical for reinforcing its trustworthiness and conveying the sense of security that users need.

Finally, the main emphasis of the business perspective with respect to the "*motivation and engagement*" is primarily to motivate and engage the crowd and all different ecosystem stakeholders via the design of an incentive mechanism that will account for intrinsic and extrinsic motives. These incentives will influence the behaviour of individuals and organisational users within the ecosystem. As such offering the right incentives to each of the different actors will ensure the active engagement and motivation of users. A key variable for the success of this process is the acknowledgement of the ecosystem evolution and the user evolution within it. Thus, designing an incentive model that accounts for the dynamic evolution of the ecosystem as well as its users is critical in order not only to foster but also to maintain the crowd motivation and engagement throughout the ecosystem lifecycle. Additionally, depending on the type and focus of the crowd-driven ecosystem, one should also account for user interactions with each other within the system. Therefore, in order to facilitate user interaction and co-creation within such ecosystems, different design logic should be applied. This will enable and encourage users to network and collaboratively contribute in the innovation development process of the given ecosystem.

4 IoT Lab: An Innovative Crowd-Driven IoT/IoE Ecosystem

IoT Lab [35] project mainly focuses on the area of Internet of Things and crowd sourcing. It is developing a research platform that combines Internet of Things (IoT) testbeds together with crowd sourcing and crowd-sensing capabilities. IoT Lab aims to enhance the existing static IoT testbed infrastructures by utilising ad hoc crowd devices (smartphones, mobile/portable devices) creating a distributed crowdsensing IoT infrastructure as well as a crowdsourcing infrastructure leveraging the collective intelligence of the crowd. By doing so IoT Lab creates an open and collaborative ecosystem for crowd-driven research and experimentation, that enables a wide range of multidisciplinary experiments. As such, it enables researchers to exploit the potential of crowdsourcing and Internet of Things testbeds for multidisciplinary research with more end-user interactions.

On one side, IoT Lab approach puts the end-users at the centre of the research and innovation process. The crowd consists the core of the research cycle with an active role in the research from its inception to the results' evaluation (crowd-driven research process) as shown in Fig. 2. It enables a better alignment of the research with the society, end-users needs, and requirements. On the other side, IoT Lab aims at enhancing existing IoT testbeds, by integrating them into a Testbed-as-a-Service (TBaaS) and by extending the platform adding crowd sourcing and crowd-sensing capabilities. To achieve such aims, the IoT Lab focuses its

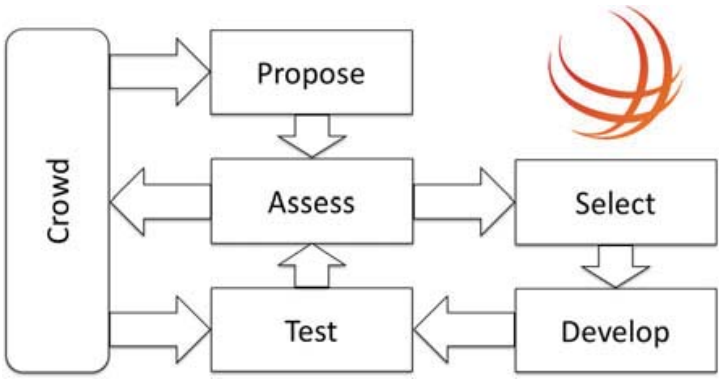

Fig. 2 IoT Lab Crowd-driven Research Process

research and development on the following areas: (a) Crowdsourcing and crowd-sensing mechanisms and tools; (b) Integration of heterogeneous testbeds; (c) Virtualisation of testbed components and integration into a Testbed as a Service; (d) Testing and validating the platform with multidisciplinary experiments; (e) Research end-user and societal value creation through crowdsourcing, and (f) "Crowd-driven research".

IoT Lab follows a multidisciplinary approach and addresses important issues such as, privacy, and personal data protection through 'Privacy by Design' approach and built-in anonymity. The IoT Lab tools include the Tesbed-as-a-Service (TBaaS) that enable, the researchers to create and manage their experiments and interact with all the available testbed and mobile resources, through a web interface. Regarding the interaction with the participants, an IoT Lab application has been developed, currently targeting the Android platform. Through this application, mobile resources from users provide both sensing information (crowdsensing), as well as, knowledge from the crowd (crowdsensing) by participating in different ongoing researches. These interactions include actions such as answering a questionnaire, annotating data, taking a picture, and sharing sensor data. The overall view of the IoT Lab as a Service is depicted in Fig. 3.

In order to analyse further the IoT Lab ecosystem, we adopt the multi-dimensional approach presented in Sect. 3. The sections that follow present an analysis of the key drivers and major challenges in its design and development of this crowd-driven IoT ecosystem.

4.1 Technical Perspective of the IoT Lab

The IoT Lab platform aims to reach beyond the notion of a static federation of IoT testbeds. More specifically, since the primal phase of its design, the role of the end-user, as well as the corresponding dynamics inferred were put in the forefront. The way the end-user would interact with the facility, the particular type of interactions supported, and the degrees of freedom the end-user would be provided by

Fig. 3 IoT Lab as a Service

the platform were carefully and thoroughly addressed. This direct interaction between the platform and its end-users posed important issues with respect to privacy, trust, and protection of the user-generated data. Another important aspect has been the design of mechanisms that successfully engage end-users into using and contributing to the platform. These aspects were considered and addressed on top of the various facility federation difficulties that have been addressed (although in a different context) by other federated facilities as well.

4.1.1 Key Technical Drivers for the IoT Lab Platform

One of the key drivers for IoT Lab has been the modern technology landscape as it has been defined after the introduction of truly portable and highly personal devices such as smartphones and smart wearables. These modern smart devices come with significant communication capabilities by supporting several wireless radio interfaces. Furthermore, the constantly evolving micro electromechanical systems (MEMS) technologies have not only changed the dimension and precision of sensors, but also their integration potential, allowing them to be installed in common mobile devices (like smartphones) and enhancing the user experience. Modern mobile phones ship with vivid screens, staggering photographic sensors, integrated GPS receivers, and a plethora of embedded context aware sensors. The increasing adoption rates of modern mobile devices by the public in conjunction with the development of smart services and the continuous evolution of advanced network technologies have paved the way for a new paradigm; namely the Mobile Crowdsensing Systems (MCS) that seek to exploit the embedded sensory capabilities of such devices carried by people in their everyday life.

In the MCS paradigm smart devices, such as smartphones, are not only regarded as data collection points but also as a direct means of interaction with their owners. In this context, the intrinsic integration of smartphone devices to the IoT Lab platform was regarded as the way to go in order to enable the facility to establish a two-way interaction scheme with its end-users. On one hand, it would enable the facility to opportunistically augment its sensing infrastructure via crowdsourcing. On the other hand, it would provide a direct and innovative way of interaction with its end-users, enabling them to provide input on their personal preferences and perception.

Apart from this novel perspective on the technical aspects of the IoT vision, the IoT Lab platform is also driven by the rapid expansion of the IoT domain that is foreseen for the coming years. Various business analysis estimate that the Internet of Things will be the largest device market in the world by 2019 and it will be more than double the size of the smartphone, PC, tablet and the wearable market combined [36]. However, currently 99.4% of physical objects that may one day become part of the Internet of Everything are still unconnected. Cisco estimates that there were about 200 million things connected to the Internet in the year 2000. Currently this number has been increased to approximately 10 billion [37]. IoT Lab seeks to leverage this infrastructure by integrating the corresponding networking technologies (LTE, Bluetooth, NFC, etc.) into a service platform that will be open and easily accessible to people and scientists.

4.1.2 Key Technical Challenges

Federating several existing experimenting facilities, each one with its own application focus and design choices under a common federated platform is already a difficult task that poses some key challenges. Although several similar efforts (i.e. federating already existing facilities) have already taken place successfully in the past, the vision of the IoT Lab to incorporate crowdsourced resources into an IoT meta-testbed demonstrates unique characteristics and, therefore, challenges. Fig. 4, the final federation architecture is depicted; in the following, we discuss the main issues that had to be addressed with a particular emphasis on privacy and trust for the crowd.

IoT Testbed Federation and Crowdsourced Resources

The main attribute of the IoT Lab architecture is modularity. Each individual experimenting facility that is about to be federated is treated as a standalone module whose details are obfuscated, via a virtualisation mechanism. In particular, each individual facility has been designed to address a different IoT domain. For example, the testbed of the University of Surrey was developed with a focus on algorithmic design and experimentation, while the testbeds of University of Geneva and the Computer Technology Institute are focusing on end-user applications for smart buildings. That said it is evident that these differences lead to significant diversions in terms of design choices, technologies used, and services provided. The virtualisation layer creates a diverse set of facilities capable of synergising with

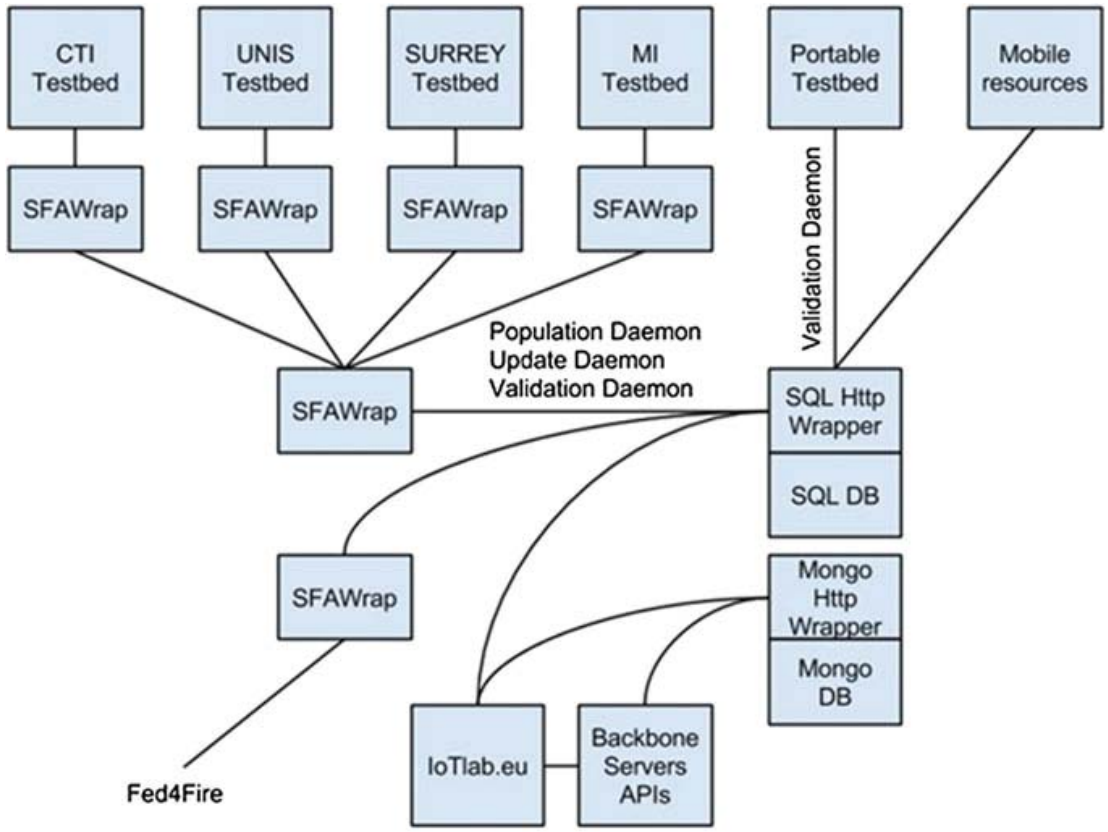

Fig. 4 The IoT Lab modular architecture

each other towards a unified platform. This is achieved via a commonly understood set of RESTful APIs used by the various modules, in order to communicate with each other. These APIs offer the services and the resources of each facility as services that can be consumed along with the necessary information needed in order to place these services in a common semantic context. For instance, each facility not only provides access to its resources (e.g. wireless sensor motes and their measurements), but also provides information on the protocols via which this access can take place (e.g. HTTP or CoAP), the type of sensors (temperature, human presence, etc.), the units the measurements are taken (e.g. Celsius degrees, binary, etc.) and other. This information follows a predefined structure, namely the RSpec format (RSpec format, GENI), which also defines the database scheme of the Resource Repository of the platform.

The same virtualisation layer is also followed by crowdsourced resources (i.e. smartphones and wearables) provided by the end-users of the facility and the general public. The challenge here has been to address the ephemeral nature of the availability of such resources, their highly volatile numbers and their highly personal nature. These aspects have been taken under consideration when extending the RSpec format, which has initially been initially designed to support regular communication networks, and later, IoT resources. The particular characteristics of crowdsourced resources also posed significant challenges with respect to storing

and managing the collected data. Addressing these challenges led to the use of a hybrid database scheme, which combines both relational and non-relational databases. In particular, a relational database was used in order to serve as a Resource Repository; that is maintaining all necessary meta-information of the available resources such as location, type, owner, availability, participation in experiments, etc. A non-relational database was used in order to store and manage the actual collected data; given the big volume of collected data, this provided for better post-experiment data processing and more efficient data management. The information stored in the two databases is correlated, by having the two databases sharing some common keys, thus providing coherence to the entire set of stored information.

Privacy/Security/Trust/Ethics

In our design and implementation, we obtain, store, and use specific data that comes from users' smartphones. For this reason, we ensure a full compliance with general personal data and privacy protection rules. In this view, any unnecessary collection of personal data should be avoided and it is ensured that any collected data is to be handled in full conformity with the applicable good practices. Our research is interested in moving further by developing, a "privacy by design" architecture. In order to achieve this, we identified certain technical measures that maximise the privacy and anonymity of the participants as well as the protection of their data, and implemented them in a holistic platform.

To achieve privacy for end-users we issue credentials to eligible participants so that they can authenticate themselves, revealing only the information they want to reveal or, simply, prove only their eligibility to provide sensor data and nothing beyond this. Our design grants the ability of sending only the fixed user information, including device identification, as well as, a general-purpose data container to receive the gathered sensor data. To prevent remote dumping of personal data, access is available only to the smartphone's resources and data for which the user has given explicit approval. The platform enables the users to fully control and change their access preference parameters at any time, including the types of data that they are willing to share. All the participants have full control on their personal data, with the rights to access, modify, delete or hide it. The platform is designed in a way that provides collaborative crowd monitoring and control of ethical and personal data protection issues. Additionally, a flag mechanism is implemented in the smartphone application that enables users to characterise, according to their opinion, an experiment as "*aiming at an unethical objective*", in case they believe the experiment violates the adopted personal data protection rules.

Since, by design, the targeted use cases do not require users to give identifying information (e.g. they can register to the platform using only a pseudonym) anonymity is preserved. However, it is necessary to anonymise the users' devices since information sent by a mobile device may lead to user identification, in some cases. Two basic assumptions are made: (i) no SIM identifying information is sent over, and (ii) we do not consider techniques that masquerade a user's IP address when interacting with the platform. The former is a use case assumption since it is not required by mobile devices using SIM cards to transmit SIM related

information. The latter assumption is made because IP masquerading and IP anti-spoofing techniques are beyond the scope of our work.

With regard to data protection, we have taken steps to provide an A*uthentication and Authorisation system*, as well as, ensuring data transmission and storage security. Persons in charge of user's data processing will be granted access electronically with special authorisation credentials and by giving them specific processing rights. These credentials will consist of an identity number and a password. Where authorisation profiles with different scopes have been defined for the persons in charge of data processing, an appropriate authorisation system will be used for access control. Authorisation profiles for each group of data processors with the same access rights will be defined and configured prior to the beginning of processing, in a way that allows access only to the data that are necessary for the processing. In order to ensure secure data transmission from users' mobile devices, we consider the deployment of TCP/IP security protocols for all data transmissions and connections. TLS/SSL protocol appears to be a good candidate to base our security solutions for all connections: Web applications connections (applications for experimenters and users to have access in their data), Android device connections (between the users' Android devices and the platform) and Testbed connections (for the interconnection between the testbeds). Furthermore, data storage is protected against any illegitimate access by external parties. We address this issue at several layers. The first layer enforces database access control, through a username/password based authentication mechanism, as well as, through imposing discrete roles for different user classes. At a second level, we implement a mechanism to disassociate data from their originators, i.e. the participating users. Finally, a data encryption layer is implemented. More specifically, we store users' personal and sensor data in separate files, with different access requirements and restrictions for each separate file. By doing so, there is no way that the sensor data (e.g. GPS position) and the socioeconomic profile (e.g. education level) of a user can be linked to the particular user through an identifying token (e.g. email), leading to lift the anonymity. In order to achieve this dissociation, the sensitive and anonymised data is stored in separate tables in a MySQL database. For additional security measurements, all database tables that store sensitive data are encrypted. Moreover, each time a new user is registered, a process with administrator privileges will decrypt the table, insert the user information and then encrypt the table again.

Motivation/Engagement

As previously mentioned, end-user motivation and engagement are crucial to crowdsourcing ecosystems. Different types of incentives are commonly used in these ecosystems in order to maximise the impact and use of the platforms. For the IoT Lab case, a combination of intrinsic and extrinsic types of incentives has been implemented. A Hybrid incentives model with gamification is followed, that allows researchers to allocate budgets for their researches. As part of the research description, the researcher is able to specify for each type of action the counterpart to be attributed to the participant, for performing such action, in the form of points. The **Incentives and Reputation framework** component of the platform, as the name indicates, is responsible for handling all the incentives-related functionalities,

that include, triggering the attribution of points when the participant fulfils a specific action. At the time a research finishes, it offers the choice to the participant to either exchange the collected points by vouchers, or to donate them to a specific charity. Those charities are selected from a list of registered and validated institutions in the platform. Another important functionality offered is the collection of badges by every user. These are acquired and collected by the users when fulfilling a specific task or achievement. The badges can be seen as an intrinsic form of incentives, but also serve as an important reputation mechanism that allows better classification and filtering of users.

4.2 Business Perspective of the IoT Lab

IoT Lab is an innovative crowd-driven IoT/IoE ecosystem that utilises the emerging participatory value creation model that is driven by users. It is an open, collaborative, user-driven, value-creating IoT ecosystem that explores the potential of crowdsensing (opportunistic and participatory sensing) and crowdsourcing to extend the IoT testbed infrastructure. In particular, IoT Lab aims to enhance the existing static IoT testbed infrastructures by utilising ad hoc crowd devices (smartphones, mobile/portable devices) creating a distributed crowdsensing IoT infrastructure as and crowdsourcing infrastructure leveraging the collective power and intelligence of the crowd. By doing so, IoT Lab creates an open, collaborative IoT ecosystem that assimilates smartphones with existing testbeds for crowd-driven research and experimentation that enables a wide range of multidisciplinary experiments.

The business perspective plays a key role in the design and development of the IoT Lab ecosystem as it facilitates the creation of a successful and sustainable hybrid crowd-driven network. In particular, it focuses upon the three key thematic areas presented above so as to ensure the creation of shared value with the given ecosystem. The sections that follow present the key drivers and challenges of the business perspective.

4.2.1 Key Business Drivers for the IoT Lab Platform

One of the key drivers for IoT Lab has been the *emerging market* that it addresses. In particular, IoT Lab explores the potential of a multidisciplinary, crowd-driven experimentation that amalgamates traditional IoT testbed infrastructures with ad hoc crowd devices, leveraging this way both the collective power and the collective intelligence (crowd capital) of the crowd. As such, understanding the demand side and identifying the market needs has been a critical aspect. The need for "crowd-sourcing driven research" has been addressed by integrating crowd capital across various experimentation phases (Fig. 5), such as: experiment conceptualisation, execution, analysis and commercialisation (optional phase).

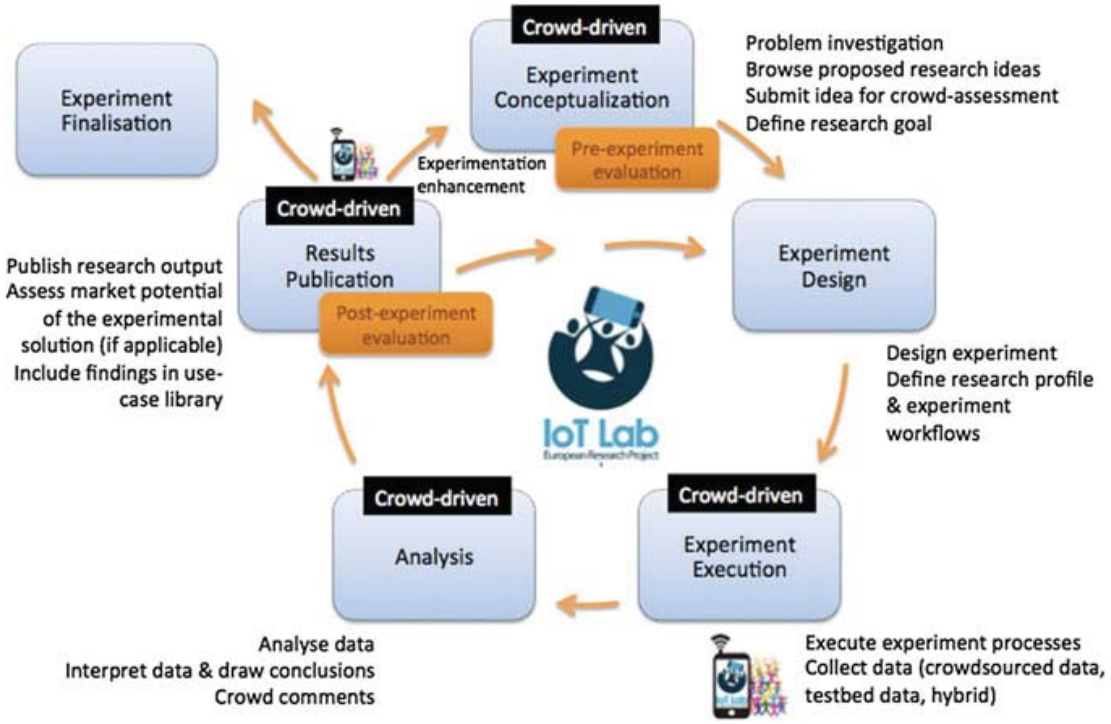

Fig. 5 IoT Lab experimentation life-cycle model

Another key driver has been the change from the users' passive role, to the active co-creators and collaborators that in conjunction with the increasing interest and ability, due to the rise of smart devices and network technologies, in actively engaging with the crowd for particular purposes (i.e., ratings, task-oriented activities, problem solving, etc.). As such, the adoption of a *user-centric participatory model* has been instigated in numerous industrial sectors. This has been fueled by the Internet of Things (IoT), the emerging technological advancements and the smart personal devices (wearables, smartwatches, smartphones, etc.) that provide the ability to harnessing both the power, and the intelligence of the crowd that can now sense, observe, measure and make sense of real-world conditions. These driving forces have been critical for IoT Lab as it focuses upon the development of a crowd-driven IoT ecosystem that encompasses all these business-level innovations in a single infrastructure providing this way a greater scope for multi-dimensional experimentation.

4.2.2 Key Business Challenges

The aforementioned drivers and IoT Lab's innovative approach provide one side of the business aspects related to this crowd-driven ecosystem. However, in order to allow a clear understanding of the implementation of the multi-dimensional model for such networks, it is vital to identify the challenges and complexities that impact their design and development.

Requirements/Needs

One of the challenges in the context of IoT Lab was the identification of market data. Lack of data, due to the emerging nature of the market that it addresses, not only hinders the ability to generate insight, but also creates a barrier to the identification of realistic market estimation. As a result of this difficulty, additional qualitative methods were utilised in order to understand the demand side and the needs and requirements of the primary users.

In addition, the creation and co-creation of value hinders a number of challenges. These are both related to the effective design as well as the management of this co-creation process [38]. Users should be provided with the necessary tools that will ensure both their connectivity as well as their ability to interact and co-create value at different levels. In the context of IoT Lab the different phases and types of crowd involvement have been defined (Fig. 3). This facilitated the design of the co-creation process and the introduction of the necessary tools (i.e., voting, assessment mechanisms, etc.) that will act as the co-creation infrastructure within this ecosystem. This infrastructure also serves as the basis for crowd interaction in the context of IoT Lab and therefore, it affects the quality of the co-creation experience between users and the ecosystem [39]. As such, by placing emphasis upon this infrastructure and its ability to create a variety of experiences for the IoT Lab users we invest in the unique value for each individual in the ecosystem, which will impact value co-creation within this ecosystem [39]. Nurturing and managing this value creation and co-creation process constitutes another key challenge. Following the DART model of value co-creation [39] we addressed this challenge in the context of the IoT Lab ecosystem. Despite the fact that this framework considers the "consumer-company interactions" we analysed its building blocks: dialogue, access, risk assessment, and transparency, in an open community environment governed by a non-profit association—the IoT Lab Association.

Emerging crowd-driven IoT/IoE ecosystems demand that we revisit not only how we create/co-create value, but also how we capture value. This constitutes another challenge for an open ecosystem such as IoT Lab. This is due to the fact that portions of value are captured by different entities in addition to the ecosystem itself. As such the identification of the appropriate business model for this crowd-driven ecosystem has been critical for its success. The identification of a business model that will account both for the value creation and the value capture elements [40] within the IoT Lab community has been critical. This is also related to the sustainability of the ecosystem, as the envisioned business model acts as the basis for the design of a sustainability model that will examine economic, community, and innovation views aiming to nurture an evolving ecosystem.

Privacy/Security/Trust/Ethics

Due to the fact that the IoT Lab ecosystem is based on crowdsourcing and crowdsensing principles, the acquisition, storage, and usage of crowd-driven data is central to its activities. As such in order to ensure compliance with personal data and privacy protection rules; a "privacy by design" approach has been followed. However, although ensuring the security and privacy within IoT Lab has been a critical aspect of its design and development process, conveying this assurance to

the crowd and the community of users creates a challenge. Reassuring users and all IoT Lab stakeholders about their data privacy and security is an aspect that significantly impacts the adoption of the ecosystem. Consequently, the establishment of the IoT Lab Association as well as introduction of policies that define among others data ownership principles within the ecosystem and rules of conduct facilitate this process. These parameters, pave the path for the creation of secure and trusted relationships and co-creation environment, as they act as an additional layer above a technically secure, privacy-aware, and trusted infrastructure.

Another business level challenge relates to the establishment of intra-ecosystem security and trustworthiness. That is security and trustworthiness at a micro-level (actor-level) that relate to the different stakeholders within the IoT Lab ecosystem. This challenge can be addressed with the design of an intra-ecosystem reputation mechanism that will increase the trustworthiness (reputation capital) of the individual actors and their activities, within the ecosystem (i.e., initiate a new crowd-driven research, etc.), which will enhance further the creation of trusted environment. Finally, transparency in the interactions between the IoT Lab Association (governance body) and the broader ecosystem community is critical for the formation of trust. In addition, the adoption of ethical practices (i.e., code of ethics) within the IoT Lab ecosystem will alleviate trust concerns of the user community and will convey a sense of security that users need.

Motivation-Engagement

Finally, another major challenge in the context of IoT Lab has been the design of an incentive mechanism that will motivate and create an active and engaged community of users. Offering the right incentives, for each actor while acknowledging the different phases of the IoT Lab ecosystem evolution, as well as, the evolution of the user himself within the system, has been a challenge. This implies the need for an incentive model that accounts for the dynamic evolution of the IoT Lab ecosystem and its users, in order to foster and maintain the crowd motivation and engagement throughout the ecosystem lifecycle. As such, updating the incentive model for the different phases of the IoT Lab is critical, as this will align with its actual community needs. Given the co-creation element of the IoT Lab special emphasis has been placed not only upon the design logic but also upon the incentives that will trigger users to network and collaboratively contribute in the crowd-driven research process.

4.3 People/End-User Perspective of the IoT Lab

In relation to IoT Lab, there are at least two main end-user groups that need to be taken into consideration in the process of developing the system. These are the crowd (i.e. the contributors) and the experimenter (i.e. the requesters). By means of IoT Lab, end-users (i.e. the crowd) can contribute to an experiment either initiated by the crowd or the experimenter community. Hence, IoT Lab must handle two different end-users' perspectives while ensuring a high level of utility, usability, and

usefulness of the platform. In this context, it is important to balance between the different drivers for each user groups while creating value for the whole eco-system. Hence, a symbiotic relationship between the three aspects of the crowd, the experimenters (requesters) and the IoT Lab platform becomes an important goal to reach. These different end-user groups are also motivated differently and thus, different incentive models focusing on creating value through the use of the IoT Lab platform should be applied.

For the end-user group of researchers, there are additional requirements that come into focus. The end-user groups' system requirements are highly connected to ensure that the collected data is reliable, trustworthy, and of high-standard quality. Moreover, the aforementioned requirements ensure that end-user groups have control over the data collection process, that the selection of respondents is easy and reliable, and that the contributors' privacy is ensured. This group of end-users is mainly motivated to use this type of system since the latter provides access to real world data that would be difficult to collect otherwise. It also enables researchers to combine new types of data and contexts, such as, levels of happiness related to a specific location. Furthermore, it enables users with limited, or lack of, technical background to perform sensor-based. Consequently, new data collection methods and research questions derive by the use this type of technology—questions that need to be tackled and answered.

4.3.1 Key People/End-User Drivers for the IoT Lab Platform

During the start-up of a crowdsourcing platform, it is important to identify the lead-users, or initiators and interest organisations, which can be motivated to be the first to participate and contribute to the crowdsourcing effort, i.e. IoT Lab platform. For these lead-users, it is important that their needs and drivers correspond to the aim of the experiments and the platform. In the case of the IoT Lab platform, the aim is focused on crowdsourced driven research, or citizen science initiated by the citizens. In the IoT Lab platform, the main driver for the crowd has been identified as a will to contribute to a better society and having fun while doing it. Societal contributions, in this case, can take different forms. It can be either through the incentive system, focusing on giving to charity, or it can be about the experiments such as contributing to a better society by, for instance, measuring air pollution or noise pollution in a specific area. Hence, the crowd is driven by idealistic ideals.

For the experimenter end-user group, drivers are somewhat different than the crowds' even though there is some overlap since both end-user groups want to create value for a common good in some sense. Among researchers, drivers, such as getting in contact with the real world and getting access to context data as they emerge, are the most prominent. IoT Lab also facilitates new interesting and challenging research areas and questions. These also become a driver for the researchers' group, as they desire to challenge established knowledge, while they explore new questions and situations.

4.3.2 Key People/End-User Challenges

When it comes to end-user challenges and the IoT Lab platform, there are several aspects that need to be considered and grapple with. We need to come up with a solution that creates value for both use sides, while offering an opportunity to the generic users to become more actively engaged in experiments and research projects and thus strengthen democracy itself. We need to stress the fact that, the experiments, their quality, and their scope are of utmost importance. Consequently, at this stage the added value of the crowds' contributions needs to be explicit and well defined. Additionally, in IoT Lab platform, the experiments must be crystal clear, engaging, and often divided into micro-tasks that are easily managed, since the crowd is characterised by limited available time and attention span. As a result, the challenges of the platform emerge on two layers: first on the usability layer of the platform and the second on the experiment layer that the crowd should contribute to. At this point, it is important to understand what users are motivated by in order to design tasks that the crowd wants to engage in.

In relation to challenges related to privacy and participatory sensing, aspects such as time, location, pictures, videos, sound samples, acceleration, environmental data, and biometric data are important and require special handle. For example, time and location is data acquired by many applications and due to their nature, these two modalities have shown to lead to privacy sensitive information about the end-users, including home and workplace locations, routines, and habits. When it comes to environmental data, for instance gas and particle concentration, it may not be a threat of privacy in itself, but when it is combined, for instance, with temperature identification of location down to a room level in a building is possible, which might invade privacy aspects in a workplace.

Based on this, we conclude that privacy threats are an inherent challenge of any participatory sensing application, especially when different sensors are combined. Hence, addressing privacy threats in this field is a multi-dimensional problem that needs to be considered and designed into crowdsourcing and IoT solutions. For instance, participatory sensing solutions should have functionalities that facilitate tailored sensing, anonymous task distribution, anonymous and privacy preserving data reporting, pseudonymity, spatial cloaking, data perturbation, hiding sensitive locations, and access control and audit. In previous studies [41–43] it has been revealed that fundamental research in the field of privacy related to participatory sensing is still in its infancy. Thus, challenges such as including participants in the privacy equation, providing adaptable privacy solution, trade-offs between privacy, performance, and data fidelity, making privacy measurable and defining standards for privacy research are important to investigate further. As of today, many end-users are rather naïve and unaware of what can be done with their data both in the primary and secondary usage of it. Hence, to succeed with crowdsourcing solutions that are ethical in their character, privacy must be protected without putting the responsibilities and efforts on the end-user side.

As a conclusion the table that follows presents the major challenges in the design and development of the IoT Lab crowd-driven ecosystem (Table 3).

Table 3 Challenges in the design and development of the IoT Lab crowd-driven ecosystem

	Technical perspective	Business perspective	People perspective
Requirements/Needs	• Resource heterogeneity (static, mobile, portable) • Testbeds integration • Modularity • Overall performance and scalability • Federation of testbeds • Integration of complex databases and Resource Directory • Scalability of platform in terms of Mobile Users and IoT Resources • Degree of Freedom for experimenters • Simultaneous direct requests to database • Simultaneous requests to Resources via main platform server. • Localizing the resources	• Market needs and data • Creation and co-creation of value • Quality of co-created value • Capturing value in an efficient way • Ecosystem sustainability	• Engaging projects for the crowd to contribute to • Quality of data • Ease of use of the system • Usefulness of the system • Ease of learning • Satisfaction • Ease of remembering
Privacy/Security/Trust/Ethics	• Privacy by design • Right to be forgotten • Disassociation of data to its owner • Physical location (country) of server and main database due to legal issues	• Reassuring users about the ecosystem privacy and security • Trusted environment & relationships/interactions • Intra-ecosystem reputation mechanisms	• Perceived trustworthiness of the system • Opportunistic sensing (coming from people) and information security • Data from sensors is involuntary • No control over data collection (what, when, where) raises serious privacy concerns • Participatory crowdsourcing • Voluntary data sharing method—individual chooses what she/he wants to report to the system

(continued)

Table 3 (continued)

	Technical perspective	Business perspective	People perspective
			• Minimal privacy concerns but no control after reporting • Important information security, integrity and availability to correct stakeholders
Motivation/Engagement	• Intrinsic motives (badges, etc.) • Extrinsic motives (money, coupons, etc.) • Implementation of incentive mechanisms—money versus badges	• Ecosystem and crowd evolution • Maintain engagement and motivation	• Understanding what motivates the crowd and their participation • Transparency in information security important for trustworthiness of the system and participation rate • Engage the crowd • Identify the right crowd • Engage crowd over a longer period of time • Transparency of data collection and use • New type of research methods

4.4 IoT Lab Crowd-Driven Ecosystem Scoring

The examination of these distinct perspectives (*people-centric, technology-centric and business-centric perspectives)* in the context of IoT Lab enabled us to identify and describe key issues that were critical for the design and development of such an innovative crowd-driven IoT ecosystem. In order to extend our analysis further, we conducted a comparative analysis of each of the three perspectives under examination by introducing the "***Crowd-driven Ecosystem Index (CEI)***". CEI measures the extent to which a holistic, multi-dimensional approach has been utilised in the design and development of a crowd-driven ecosystem initiative in the context of IoT/IoE; conveying this way its potential propensity of success (Table 4). The CEI is a quantitative measure, that acts as a self-evaluation tool and which varies between 0 and 1 and obtains its maximum value when all parameters and key thematic areas presented above exhibit highest coverage intensity. High values (CEI = 1 − 0.67) indicate that emphasis has been placed upon the different ecosystem elements, indicating a relatively high success potential of the ecosystem; moderate values (CEI = 0.66 − 0.33) indicate moderate potential; and low values (CEI = 0.32 − 0) indicate low potential.

The overall IoT Lab evaluation indicates that a balanced approach has been followed in the design and development of the ecosystem with a CEI of 0.87 (Fig. 6). The comparative results from each perspective indicated that although high coverage intensity has occurred, the values vary slightly between the different perspectives and the emphasis placed on each. As such "motivation and engagement" seems to be the thematic area with the highest coverage intensity followed by requirements and user utility. This is the case for both the people and business perspectives showing clearly the differences between the different perspectives.

Table 4 Crowd-driven Ecosystem Index (CEI)

Thematic areas	Perspectives			Thematic areas score
	Technical	Business	People	
Requirements/needs	5	4	4	13
Privacy/security/trust/ethics	4	4	4	12
Motivation/engagement	4	5	5	14
Perspective Scoring[a]	13	13	13	

[a]Scoring scale: 1–5, depending on the coverage intensity of each factor: (1) low coverage intensity, (2) moderate low, (3) moderate, (4) high and (5) extreme coverage intensity

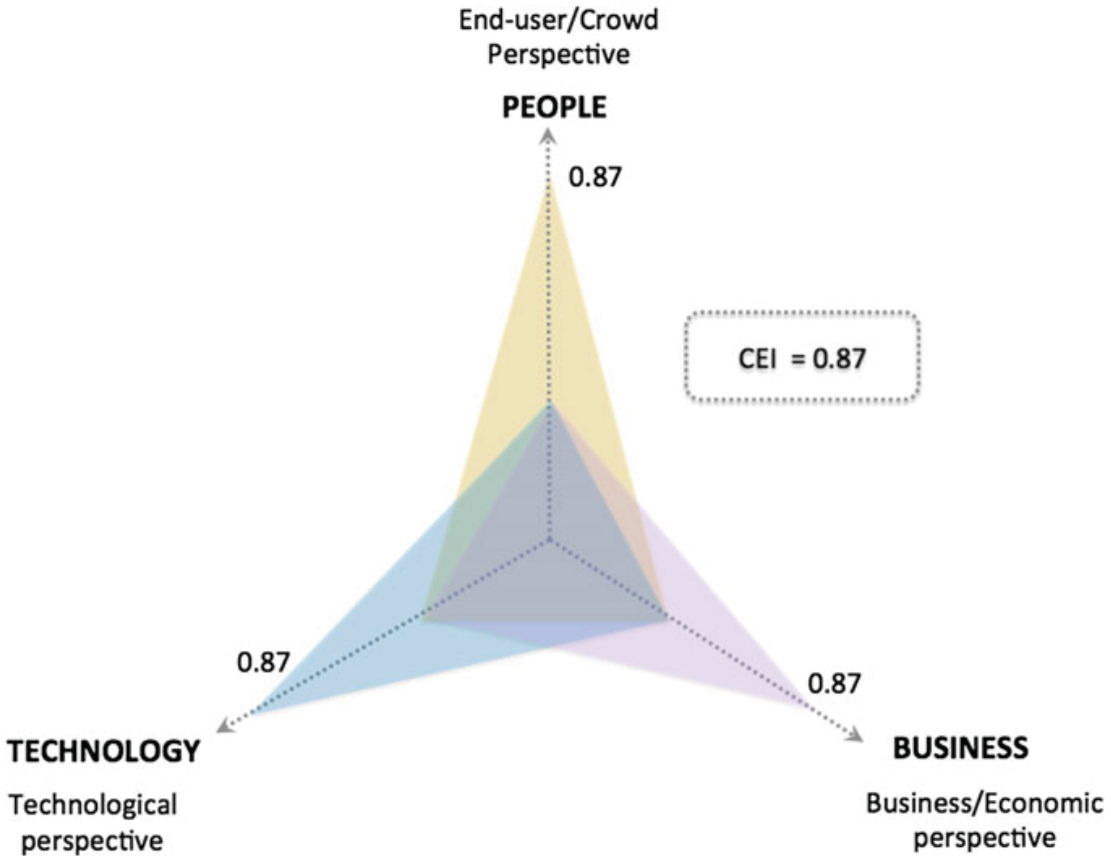

Fig. 6 The IoT Lab CEI

5 Conclusions

Crowd-driven ecosystems serve as a global meta-environment for leveraging the network effects, in order to harness the collective and distributed power and intelligence of our society. These open, collaborative, user-driven, and value creation ecosystems enable individuals to collaborate in innovative ways. Participants openly share their ideas, data, best practices, and create new knowledge that enhances our common innovation potential. This ability to exploit the capacity of the crowd has been fuelled by the Internet of Things (IoT)/Internet of Everything (IoE), introducing new user-centric paradigms, such as mobile crowd sensing (MCS). MCS goes beyond traditional sensing techniques (e.g., sensor networks, etc.,) leveraging both the power and the wisdom of the crowd in order to sense, observe, measure and make sense of real-world conditions (e.g., environmental, etc.,), and activities (e.g., personal activities and interactions, etc.,) using user-owned mobile and wearable devices. Such *crowd-driven IoT/IoE ecosystems* can exist in many forms concentrating on specific crowd-driven functions (crowdsourcing, crowdsensing, crowdfunding, etc.,) or they can be hybrid not tied to a specific mode.

Despite the promising participatory value creation paradigm and the numerous advantages it provides, crowd-driven IoT/IoE ecosystems are still in their initial

stages and face many challenges. One of the aforementioned challenges of these ecosystems relates to their design and development, acknowledging that their nature necessitates the adoption of multi-disciplinary perspectives. The existing literature emphasises the technical aspects for the development of such networks and provides useful insights of what needs to be addressed. However, the directions on the way one should design and undertake this process—accounting for non-technical ecosystem elements are limited. Consequently, there is a need for a unified framework that embraces a holistic approach to address different parameters, crucial for the design and development of such crowd-driven ecosystems. Aiming to fill this gap, this chapter provided a framework that adopts a holistic multi-perspective approach that facilitates the design and development of crowd-driven ecosystems. Our model provides three perspectives: (a) *the people-centric perspective* that encompasses the crowd views and needs for the creation and co-creation of value within a given network; (b) *the business-centric perspective* that emphasises the creation of economic and business value of a given crowd-driven ecosystems—factors that affect the network sustainability—and (c) *the technology-centric perspective* that focuses on the technological aspects (e.g., ecosystem architecture and components, technological resources, etc.) relevant to the design and development of a crowd-driven network.

The examination of this model has been implemented in the context of a hybrid crowd-driven IoT/IoE ecosystem, namely *IoT Lab* (which integrates both crowdsourcing and crowdsensing elements). IoT Lab is an innovative crowd-driven IoT/IoE ecosystem that utilises the emerging participatory value-creation model and explores the potential of crowdsensing (opportunistic and participatory sensing) and crowdsourcing to extend the existing IoT testbed infrastructure. IoT Lab is the first experimenting facility designed to not only federate several IoT testbeds, but also to intrinsically integrate crowdsourced devices as experimenting resources. This new type of resources posed new, non-trivial challenges, which have not been addressed in the past in the context of experimenting facilities. In particular, their highly personal nature (i.e. the fact that each device is owned by a person) has raised significant reliability and availability issues. This type of resources cannot be provisioned as traditional IoT resources, as the owner of the device needs to consent to their use in the context of an experiment. This way, a new ecosystem of interactions has emerged in which an experimenter, a testbed provider, and the devices' owners need to synchronise with each other, while providing the necessary guarantees. For instance, on one hand the experimenter and the testbed provider need to provide sufficient guarantees to the crowd with respect to privacy, security, and trust, while on the other hand, the device owner needs to be trustworthy, in terms of availability.

This triangle of relations' paves the way for new modes of value creation and value capture within such ecosystems, as well as, new sources of value creators and co-creators. This, however, also hinders a number of challenges related to the effective design and the management of this co-creation process. However, the emerging crowd-driven IoT/IoE ecosystems, such as IoT Lab, demand that we not only revisit the way one creates/co-creates value, but also, how value is captured.

This constitutes another challenge for open ecosystems such as IoT Lab. This is due to the fact that portions of value are captured by different entities in addition to the ecosystem itself. Hence, the identification of the appropriate business model for this crowd-driven ecosystem has been critical for its success and sustainability. In addition, many challenges need to be tackled, in order to keep people's motivation and engagement towards this type of platform. Thus, by understanding the incentivising and the driving forces of people will allow us to develop innovative engaging techniques. This will help us to motivate people to contribute on our projects on regular basis.

Our examination of these distinct perspectives (*people-centric, technology-centric and business-centric)* in the context of IoT Lab enabled us to identify and describe key issues that are critical for the design and development of such innovative crowd-driven IoT/IoE ecosystems. This has been further extended with the introduction of the *"Crowd-driven Ecosystem Index (CEI)",* which measures the coverage intensity of each of the key ecosystem parameters, denoting this way the propensity of success of a given crowd-driven network. Our comparative analysis in the context of IoT Lab indicated that a balanced approach has been followed (CEI = 0.87) with relatively high coverage intensity of the model parameters.

Some future research areas, from a technical perspective, include the use of novel privacy preserving mechanisms in the context of crowdsensing (e.g. differentially private mechanisms), providing the services and the technological enablers to support new economic models (e.g. schemes of open and collaborative economies) as well as, providing services that would further leverage the usage of crowdsourced infrastructure (e.g. in network data processing, in-memory databases for smartphones, etc.). In addition, further empirical validation of the proposed model would be appropriate in order to fine tune its key thematic areas and account for additional micro-level factors. This could also be extended with an evaluation tool that will accompany the model and provide additional guidance in relation to the design and development of crowd-driven ecosystems in the area of IoT/IoE.

Acknowledgment The research reported in this paper has been supported by the EU/FIRE IoT Lab project—STREP ICT-610477.

References

1. IEEE-IoT 2015. Towards a definition of the Internet of Things (IoT). Revision No. 1– Published 27 May 2015.
2. J. Bradley, J. Barbier, and D. Handler D. Embracing the Internet of Everything to capture your share of $14.4 trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience. White Paper Cisco, 2013.
3. J.A. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy; et al., Participatory sensing. Center for Embedded Network Sensing. 2006. UCLA: Center for Embedded Network Sensing.
4. R. K. Ganti, Y. Fan and L. Hui, Mobile Crowdsensing: Current State and Future Challenges, IEEE Commun. Mag., 49(11), 2011, pp. 32–39.

5. A.G. Tansley. The use and abuse of vegetational concepts and terms. *Ecology,* 16, 1935, pp. 284–307.
6. World Resources Institute (WRI). World Resources 2000–2001: People and ecosystems: The fraying web of life. Report Series by United Nations Development Programme, United Nations Environment Programme, World Bank and World Resources Institute - September 2000.
7. R.A. Frosch, and N.E. Gallopoulos, Strategies for Manufacturing. *Scientific American*, 261 (3), 1989, pp. 144–152.
8. J.F. Moore, Predators and prey: A new ecology of competition. *Harvard Business Review*. 71 (3), 1993, pp. 75–83.
9. J. F. Moore, *The Death of Competition: Leadership & Strategy in the Age of Business Ecosystems*. 1996, New York, Harper Business.
10. H.W. Chesbrough and M.M. Appleyard, Open Innovation and Strategy. *California Management Review*, 50(1), 2007, pp. 57–76.
11. P. Almeida and B. Kogut, Localization of knowledge and the mobility of engineers in regional networks. *Management Science*, 45, 1999, pp. 905–917.
12. R. Baptista, Clusters, innovation and growth: a survey of the literature. In: G. M. P. Swann, M. Prevezer and D. Stout, eds. *The dynamics of industrial clusters: international comparisons in computing and biotechnology,* 1998. Oxford: Oxford University Press 13–51.
13. D. Bray, Knowledge Ecosystems. In *Organizational dynamics of technology-based innovation: Diversifying the research agenda*, 2007 (pp. 457–462). Springer US.
14. T. Coughlan, Enhancing Innovation through Virtual Proximity. Technology Innovation Management Review, 4(2), 2014, pp. 17–22.
15. B. Clarysse, M. Wright, J. Bruneel, and A. Mahajan, Creating value in ecosystems: Crossing the chasm between knowledge and business ecosystems. *Research Policy*, 43(7), 2014, pp. 1164–1176.
16. G. Koening, Business Ecosystems Revisited. Management, 15(2), 2012, pp. 208–224.
17. K. Valkokari, Business, Innovation, and Knowledge Ecosystems: How They Differ and How to Survive and Thrive within Them. *Technology Innovation Management Review*, 5(8), 2015, pp. 17–24.
18. M. Iansiti and R. Levien, *The Keystone Advantage: What the New Dynamics of Business Ecosystems Mean for Strategy, Innovation, and Sustainability*. Boston, MA: Harvard Business School Press, 2004.
19. J.B. Andersen, What Are Innovation Ecosystems and How To Build and Use Them. *Innovation Management*, 2011.
20. M. Wright, Academic entrepreneurship technology transfer and society: Where next? Journal of Technology Transfer, 39(3), 2013, pp. 322–34.
21. E.G. Carayannis, Innovation, Technology, and Knowledge Management, 2010.
22. S.M. Lee, D.L. Olson and S. Trimi, Co-Innovation: Convergenomics, Collaboration, and Co-Creation for Organizational Values. Management Decision, 50(5), 2012, pp. 817–831.
23. D. Tapscott and A.D. Williams. *Wikinomics: How mass collaboration changes everything*. 2008, Penguin.
24. M. E. Porter and M. R. Kramer, Creating Shared Value, *Harvard Business Review,* 89(1–2), 2011, (January–February).
25. R.K. Rana, C.T. Chou, S.S. Kanhere, N. Bulusu, and W. Hu, Ear-Phone an End-to-End Participatory Urban Noise Mapping System. In Proceedings of the 9th *ACM/IEEE International Conference on Information Processing in Sensor Networks*, Stockholm, Sweden, 12–16 April 2010, pp. 105–116.
26. N. Thepvilojanapong, T. Ono, and Y.A. Tobe, Deployment of Fine-Grained Sensor Network and Empirical Analysis of Urban Temperature. *Sensors*, 10, 2010, pp. 2217–2241.
27. Ludwig, T., Siebigteroth, T., and Pipek, V., 2014. CrowdMonitor: Monitoring Physical and Digital Activities of Citizens During Emergencies. *Social Informatics*, 8852, pp. 421–428.
28. Bélanger, F. and Crossler, R. E. 2011. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly,* Vol. 35, No. 4, pp. 1017–1041.

29. Hong, W. and Thong, J. Y. L. 2013. Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly,* 37(1), pp. 275–298.
30. Muhdi, L. and Boutellier, R. 2011. Motivational Factors Affecting Participation and Contribution of Members in Two Different Swiss Innovation Communities. *International Journal of Innovation Management,* 15(3). pp. 543–562.
31. Brabham, D. C. 2010. Moving the Crowd at Threadless. *Information, Communication & Society,* 13(8), pp. 1122–1145.
32. Kaufmann, N., Schulze, T. and Veit, D. 2011. *More Than Fun and Money. Worker Motivation in Crowdsourcing – a Study on Mechanical Turk.* AMCIS2011.
33. Nov, O., 2007. What Motivates Wikipedians. *Communication of the ACM,* 50(11) pp. 60–64.
34. Ståhlbröst, A., Angelopoulos, C. M., Evangelatos, O., Krco, S., Nikoletseas, S., Raptis, T. and Ziegler, S., 2015. *Understanding Modes of Crowdsourcing and Related Crowd Motivators.* XXVI ISPIM conference, Budapest, Hungary.
35. IoT Lab project. Available at (access: 20.01.2016): www.iotlab.eu.
36. Greenough, J., 2014, How the Internet of Things market will grow, Business Insider. Available at (access: 25.01.2016): http://uk.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10?r=US&IR=T.
37. Dave Evans, The Internet of Everything – Cisco. Available at (access: 25.01.2016): https://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf.
38. Payne, A.F., Storbacka, K. and Frow, P., 2008. Managing the co-creation of value. *Journal of the academy of marketing science*, 36(1), pp. 83–96.
39. Prahalad, C. K. and Ramaswamy, V., 2004. Co-creating unique value with customers. *Strategy & leadership*, 32(3), pp. 4–9.
40. Chesbrough, H., 2007. Business model innovation: it's not just about technology anymore. *Strategy & leadership*, 35(6), pp. 12–17.
41. Christin, D., Reinhardt, A., Kanhere, S. and Hollick, M. 2011. A Survey on Privacy in Mobile Participatory Sensing Applications. *The journal of systems and software,* 84. pp. 1928–1946.
42. Huang, K. L., Kanhere, S. S. and Hu, W. 2010. Preserving Privacy in Participatory Sensing Systems. *Computer Communications*, 33(11). pp. 1266–1280.
43. Weber, R. H., 2010. Internet of Things – New Security and Privacy Challenges. *Computer Law & Security Review,* 26(1). pp. 23–30.