9-2017

Investigating The Business Potential Of Internet Of Things

Panagiota Papadopoulou
National and Kapodistrian University of Athens, peggy@di.uoa.gr

Kostas Kolomvatsos
National and Kapodistrian University of Athens, kostasks@di.uoa.gr

Kyriaki Panagidi
National and Kapodistrian University of Athens, kakiap@di.uoa.gr

Stathes Hadjiefthymiades
National and Kapodistrian University of Athens, shadj@di.uoa.gr

Recommended Citation

Papadopoulou, Panagiota; Kolomvatsos, Kostas; Panagidi, Kyriaki; and Hadjiefthymiades, Stathes, "Investigating The Business Potential Of Internet Of Things" (2017). *MCIS 2017 Proceedings*. 33.
http://aisel.aisnet.org/mcis2017/33

INVESTIGATING THE BUSINESS POTENTIAL OF INTERNET OF THINGS

Panagiota Papadopoulou, Kostas Kolomvatsos, Kyriaki Panagidi, Stathes Hadjiefthymiades
Department of Informatics and Telecommunications
National and Kapodistrian University of Athens, Athens, Greece
{peggy, kostasks, kakiap, shadj}@di.uoa.gr

Abstract

Internet of Things (IoT) encompasses a wide range of devices and technologies which cumulatively shape a new environment with unprecedented business prospects. This paper aims to investigate the business potential of the IoT, examining the opportunities it offers as well as the challenges it creates for current and future business models. In this direction, the paper presents a proposed framework for analyzing IoT business models into dimensions that can facilitate our understanding of their development and success. The paper also denotes factors that can affect the success of IoT business models, focusing on security, privacy, trust, legal and economic aspects of IoT. The paper continues to show the business applicability of IoT through the case of RAWFIE project, describing example application scenarios of mobile IoT in selected domains and analysing its business potential.

Keywords: Internet of Things, mobile IoT, business model, Unmanned Vehicles

1 Introduction

The Internet of Things (IoT) creates an emerging new era of the Internet, in which machines and objects get connected and equipped with sensors, surpassing their traditional role to constitute dynamic actors of networked environments with novel products and services. The ubiquitous nature of IoT brings dramatic changes to the way we work and live, with an increasing adoption in various domains, such as energy, healthcare and transportation. According to industry reports, IoT is a very promising technology and is predicted to flourish within the next years (BI Intelligence, 2016). It is expected that more than 24 billion IoT devices will exist by 2020, which will be four times the world population, while by 2018 IoT penetration will cover half of the world population. Investments on IoT are predicted to reach $5-6 trillion (Newman, 2017) with $13 billion estimated ROI (BI Intelligence, 2016). The IoT market is still in its infancy, with its potential yet to be revealed. More than half of major new business processes and systems will incorporate some elements of IoT (Gartner, 2017). The aim is to increase the positive impact to people’s lives and incorporate business models with increased revenues while the cost of instrumenting things is reduced.

In the IoT world, every object can potentially be a smart device, generating, processing and exchanging data, thus serving as an active participant of an intelligent ecosystem. The interconnected autonomous nodes that are capable of interacting with their environment and perform simple processing tasks allow the support of various intelligent applications. With the appropriate business models, IoT can fuel the development of new products and services that could be offered to end users. IoT technologies offer vast opportunities to build business models forming a very dynamic environment in almost every application domain. The transformational power of IoT technologies will heavily affect peoples’ lives. End users will have the opportunity to enjoy a wide range of innovative products and services by interacting with small, yet, intelligent devices capable of reasoning on the data that collect from their environment.

A new trend in the IoT is the involvement of mobile devices instead of static ones. Usually, mobile devices are unmanned vehicles - UVs (i.e., UxV, where x stands for surface, ground, aerial). The addition of mobile smart nodes further enhances the IoT potential for applications and business models. At the same time, the mobile IoT paradigm introduces many different technical challenges that call for efficient solutions either horizontally (application-neutral) or vertically (application-specific). Such challenges are faced continuously by researchers and innovators worldwide and impose different constraints for developing business models on top of numerous mobile IoT devices. For instance, mobile IoT energy resources (e.g., battery) are limited and can suffer from depletion which means that mobile IoT nodes need to have idle time for charging and maintenance and therefore cannot be constantly active and at service. In addition, mobile IoT infrastructure is prone to network connection problems, making data exchange unreliable, as there are limitations regarding the distance of the mobile nodes from the base station as well as the distance among mobile devices. Such characteristics of mobile IoT can pose new additional requirements for business models.

Although IoT has received significant research attention, most studies focus on technical aspects, either in software or in hardware. Several research efforts have studied business models in IoT, however, they are mainly focused on specific areas such as supply chain management (Papert and Pflaum, 2017) or e-business (Zhang and Wen, 2017). In addition, despite the extant literature on IoT business models, research on mobile IoT and related business models is scarce. Current literature focuses on the study of case-specific or application-specific business models limiting the potential generalizability to cover multiple IoT domains, including the mobile IoT and its special characteristics and requirements. There is a need for defining a set of dimensions that can assist in understanding and designing business models in the IoT world.

In this paper, we aim to explore the potential of IoT business models and, accordingly, to focus on the mobile IoT. The paper attempts to address the need for understanding the business potential of IoT as it extends to mobile IoT and the issues associated with its adoption, with regard to the opportunities as well as the challenges emerging from IoT technologies. We propose a framework through an analysis into dimensions for understanding the potential of IoT across application domains and the respective business models that could be developed. Business elements and a SWOT analysis at a general level are combined serving as a basis for generating and assessing potential business models and their specific characteristics. Our aim is to reveal the parameters that are critical for establishing business models that will generate revenue on top of the huge infrastructure of IoT in various domains. In this vein, we proceed with a discussion of issues related to IoT and its adoption, such as security, privacy and trust as well as economic, legal and technical issues and how in turn they can affect IoT business value. We suggest a set of technical as well as non-technical factors that should be taken into consideration and addressed for IoT business models and applications. Focusing on mobile IoT, we provide our experience from the RAWFIE (Road-, Air- and Water-based Future Internet Experimentation) project that provides research and experimentation facilities through the ever-growing domain of UxVs. RAWFIE acts as a showcase of the applicability of mobile IoT through a set of use cases. Our aim is to illustrate the application and business potential of mobile IoT by providing a description of application scenarios and discussing possible business models in the field.

The structure of the paper is as follows. Section 2 presents the related work while Section 3 presents a proposed framework analyzing the dimensions and characteristics of business models that can be realized in the IoT. In Section 4, we discuss IoT technical and non-technical success factors. In Section 5, we present the case of RAWFIE project, providing a set of examples that report on the potential of IoT business models in specific domains. Section 6 explores RAWFIE from a business model perspective and finally, in Section 7, we conclude our paper and give our future research plans.

2 Related Work

IoT can be adopted in various application domains, which can be classified according to the type of networks, coverage, scalability management, heterogeneity, users' involvement and impact (Gluhak et al., 2011). Four categories of IoT application domains have been identified by Gubbi et al. (2013):

(i) personal and home applications: personal information is collected by users' personal devices in any place. Intelligent applications are delivered on top of the collected data that are fully adapted to users' characteristics and the dynamics of the environment;

(ii) enterprise applications: the information is collected by enterprise networks and intelligent applications are delivered in domains like environmental monitoring (Abdulah et al., 2008; Gouveia & Fonseca, 2008; Hardas et al., 2008; Hatzikos et al., 2007; Kolomvatsos et al., 2015a; Kolomvatsos et al., 2015b), smart environment IoT (Gluhak et al., 2011; Li et al., 2011);

(iii) utilities: they involve intelligent applications on top of information retrieved by networks adopted to produce solutions for service optimization. Typical examples are the Smart Grid and smart energy management applications (Erol-Kantarci & Mouftah, 2010; Gao et al., 2012; Pedrasa et al., 2010);

(iv) mobile applications: these applications are built on top of the information conveyed by mobile nodes. A smart transportation system (Al-Sakran, 2015; Chepuru & Rao, 2015; Katiyar et al., 2011; Xiao, 2011), is the typical representative of such applications.

Mobile IoT involves moving devices equipped with processing and communication capabilities. The adoption of such devices has the advantage of covering larger areas than 'typical' IoT settings where nodes are static. The movement of the devices intensively incorporates, among others, the spatial aspect in the data gathering and processing. Mobile IoT scenarios (e.g., a Smart City) is characterized by short and recurrent contact between IoT devices to complete the assigned tasks (Valarmathi et al., 2016). All modern devices are equipped with Wireless technologies facilitating the creation of a vast communication infrastructure. For instance, users can connect to the infrastructure through their smartphones, cars or other personal devices. The involvement of a high number of users and the huge infrastructure makes more intense the need for handling security issues. Therefore, it is imperative to provide security measures for IoT devices that provide a potential entry point to the in-vehicle network (Oka et al., 2014).

Multiple business models have been proposed in the IoT (Chan, 2015). Fleisch et al., (2014) build on top of the analysis of 55 IoT business model patterns discussed in Gassmann et al., (2013), focusing on the value creation steps that will ensure the success of business models. The results indicate that business model patterns could be depicted by six components while defining two independent business model patterns, digitally charged products and sensors as a service. Gierej (2012) develops a business model for companies implementing technologies for industrial IoT. The industrial setting imposes various requirements in the envisioned models. The author presents the phases of the industrial Internet evolution and discusses the key roles in such a setting. Ju et al. (2016) aim to develop a generic business model framework for IoT businesses through literature analysis and interviews. A set of case studies are adopted for testing purposes in IoT companies and the findings suggest that the capability for data analytics is an essential element for IoT service. These results identify the significance of analytics services that will be proposed on top of the IoT infrastructure as they offer a uniform 'view' on the data collected by the smart IoT devices. Other findings indicate that open ecosystems help companies to provide new integrated services and offer greater value for consumers.

Turber et al., (2014) propose a framework for designing business models for IoT in a structured and actionable way, based on the result of 34 case studies. Liu & Jia (2010) propose a traditional value based business model applied for IoT applications, aiming to identify how the value is created and exchanged between actors. Fan & Zhou (2011) propose an e3-value methodology applied to the traditional business model for IoT applications. The main focus of the business model elements is on value proposition and target customers. Berkers et al. (2013) adopt a value net analysis for proposing a business model in IoT through a case study related to real-world traffic data that are generated by IoT services. Glova et al. (2014) describe the application of a value based approach to business modeling in IoT. They also apply an e3-value methodology for a sustainable business model for the IoT.

Shi (2014) studies existing business models and proposes a strategy for using business models in the development of IoT for China mobiles. The strategy includes four aspects, firstly they have concentrated on the improvement of high-quality network for IoT, secondly, they established the value proposition, thirdly they build the key partnerships, and finally key activities for launching the IoT product were discovered. Bucherer & Uckelmann (2011) propose business models for the value and revenue creation in the IoT. He et al. (2010) focus on a model to describe the impact of IoT on materials, information and capital flow for supply chain innovation. Finally, Leminen et al. (2012) categorize the business models for IoT in the manufacturing industries. The authors describe the challenges like unprofitable environment, exploded market and need to extract more value in the existing business models for IoT and established a framework to identify different IoT business models. In general, a set of challenges in designing IoT business models have been identified (Westerlund et al., 2014):

- *Diversity of things*. This challenge involves the heterogeneity of the things involved in IoT like the devices. Such devices coming from different manufacturers convey different ways for ‘annotating’ the information, thus, affecting the way they are connected together.
- *Immaturity of innovation*. IoT is a hot research and business area, thus, the number of the emerging technologies is huge. Standardization activities are in their infancy affecting large scale deployments. In addition, the connection of the IoT technologies together is very difficult due to the different formats and schemes adopted to ‘annotate’ the data and the devices themselves.
- *Unstructured ecosystems*. The current form of IoT lacks specific roles for stakeholders. New business models demand creating new relationships in new industrial sectors, extending existing relationships and penetrating new sectors. The complexity of an ecosystem is related to the number of participants and IoT is still not mature (UNIFY-IoT, 2016).

3 An analysis framework for IoT business models

This section proposes a multi-faceted framework for the classification and analysis of IoT from a business perspective. IoT applications can be analyzed into a number of dimensions that can separately and jointly describe the business characteristics and aspects of IoT. IoT is an infrastructure of interconnected objects, whose architecture is different from that of the traditional network, which cannot simply be described by the use of the layered network architecture (Wang & Wu, 2011). In order to allow for a deep understanding of the IoT potential, that will facilitate the exploration of how IoT can enable the development new business models and value creation, IoT is proposed to be analyzed into certain dimensions regarding its context, users, stakeholders, purpose and the benefits it offers, which are presented below in Table 1 along with an analysis of the strengths, the weaknesses, the opportunities and the threats associated with the IoT use. These dimensions represent characteristics that are general for IoT and its applications and can serve as pillars for conceptualizing and evaluating potential IoT business models. Dimensions are selected as they can be deemed as a broader, more generic version of business model building blocks, such as those suggested by Osterwalder & Pigneur (2010). In this direction, they can be used as a starting point for defining specific business model elements, such as value proposition, infrastructure, customers and finances, when generating IoT business models.

Dimensions	Values
Users	Individuals
	Companies/businesses
	Governments, public organizations, non-profit organizations, NGO
Stakeholders	Device manufacturers
	Network operators
	Service providers
	Infrastructure providers
	End users
Purpose	Profit
	Non-profit/Commonwealth
Context/Level	Individual
	Organizational
	Community/Society/Public
Benefits/Value	Monitoring and control in real time
	Cost reduction
	Automation of processes – human disintermediation
	Increased productivity
	Improved quality of life
	Enhanced communication infrastructure for access and connectivity
Strengths	Dynamic, real-time, adaptive function
	Context-specific applications
	Location independence
	Rich data
	Mobile, remote management
Weaknesses	Security
	Privacy
	Trust
	Interoperability
	Lack of standardization in communication protocols
	Energy/autonomy
Opportunities	IoT market in its infancy
	IoT hardware cost drops
	Large investments and ROI expected
	High degree of practical applicability in various sectors
	Applicable in many everyday widely used objects
Threats	Security attacks
	Technological immaturity of data exchange protocols
	Heterogeneity of objects and devices
	Lack of vendor independence

	Immaturity for management (storage and processing) of huge amounts of data
	Immaturity of adoption at individual level
	Legal/regulatory framework

Table 1: IoT business dimensions

IoT can be applied in numerous domains at individual, organizational or society/public level. The users of IoT ecosystems can be individuals, businesses or other organization types, and governments, with IoT use being for profit but also for public commonwealth purposes. Key stakeholders involved in IoT business models are device manufacturers, infrastructure providers, network providers, service providers and end users. IoT brings several benefits horizontally across application domains, such as real-time monitoring and control, human-less automated processes and cost reduction. IoT strengths include its dynamic, real-time, context-specific functionality, enabling rich data collection and location independence. IoT offers many business opportunities as the IoT market is still in its infancy with large expected investments and a wide range of possible applications in various objects and sectors. However, IoT comes with weaknesses such as security, privacy and trust. In addition, IoT can be threatened by factors such as the immaturity of data exchange and management, the heterogeneity of IoT components and the inadequate legal and regulatory framework.

The proposed framework can help enhance our understanding of IoT applicability and potential and serve as a tool for identifying the possibilities for IoT business models as well as the challenges that should be addressed in any application domain. IoT horizontal benefits, in conjunction with its strengths, can be vertically applied and analyzed into domain-specific benefits. Similarly, the IoT promise comes with several weaknesses and threats that cannot be neglected in developing business models, which are vertically applied for each application domain.

4. Assessing IoT success factors

Internet and the Web have had a significant impact on business models over the past two decades, which can be distinguished into three phases (Fleisch et al., 2014). The Web 1.0 era was characterized by the substitution of the physical elements with the virtual, and the value of the online channel to a business model. Internet and the Web are used as the business infrastructure or as part of it and the power shifts from the business to the consumer. In Web 2.0, the value stems from the users and/or customers who become key assets to business models, as they are content providers and form a social network oriented market with collective power. Sharing is a core asset of business models, as relevant activities are delegated from the business to the users, and interaction is further enhanced with social media and mobile devices such as smartphones and tablets.

Various efforts are present in the respective literature that deals with the success factors of IoT business models (Martin, 2015; Srini, 2016; Swanepoel, 2016; Wilhite & Mehraban, 2015). Unfortunately, these efforts focus on the high level strategies that could be adopted towards the successful conclusion of a business model. This ‘generic’ approach should be enhanced by issues that affect the inclusion of any business model in the everyday activities of end users. Important aspects of IoT applications should be taken into consideration before they are in a position to be included in users’s lives. In this section, we try to reveal all these issues and provide a comprehensive insight on the significant aspects of IoT applications.

IoT leads towards the next wave of IT-enabled business models, in which the value lies in the merge of the physical and the digital, with a hybrid ubiquitous infrastructure of smart devices that can have processing power, sensors, network connectivity and location awareness. The value proposition is complex to determine, including if it refers to a product or a service, as the product and the service are now integrated into a bundled smart object. Data generation, exchange, storage and analysis emerge as critical success factors for IoT applications as they constitute the basis for the value creation of IoT business models. The amount and richness of the sensor-driven data that can be made available through networks of connected devices can support numerous activities in diverse contexts, offering tremendous business opportunities.

In this setting, IoT can create value for new business models and upgrade the value for existing ones. IoT technologies can provide a dynamic ecosystem empowering numerous actors and applications in diverse sectors with multiple beneficiaries. However, the power of these technologies cannot be harnessed without taking into account the risk inherent almost in every possible use of IoT technologies. In this direction, we take a closer look on the weak and threatening factors of IoT business applicability mentioned in the proposed framework, focusing and elaborating on the socio-technical aspects of security, privacy and trust, as well as economic and technical issues.

Security has always been a principal factor for almost every kind of technology adoption. In IoT, existing and well-known security issues remain important to be tackled with, while new IoT-specific security risks and challenges are introduced, at both physical and digital level, associated with devices, platforms, operating systems and power. In this setting, organizations should deploy security strategies, principles and technologies that are flexible to evolve and adapt to new threats. The successful development of any IoT systems lies in the proper awareness and knowledge of IoT security issues. A security approach is indispensable for any IoT business model. Security should be identified as a key aspect of the design and implementation of IoT systems and should be incorporated in all stages of their lifecycle.

The design and deployment of IoT applications should also be considered with respect to privacy and the unauthorized collection and use of data. Data protection and privacy issues are not domain-specific and can be of critical importance to any application in any sector. Especially, in certain areas, like healthcare, these issues are extremely vital to human-centric activities involving personal data and therefore have to be carefully considered and addressed, otherwise they will be an impediment to the development and successful adoption of IoT applications. This is a challenge that has to be tackled at both industry and government level.

Another important factor that can influence the wide acceptance of IoT in personal as well as organizational activities is trust. Extending the security and privacy issues that need to be tackled, the lack of trust in the IoT and their applications can also be an inhibitor of IoT adoption. Thus, it is necessary to ensure that any IoT application can be trusted by the intended users. Trust building in IoT can be mainly approached in two ways. The first approach is to foster trust in IoT by raising awareness regarding the security and privacy risks associated IoT use and informing interested parties about the possible solutions towards the effective management of these risks. The second trust-building approach involves facilitating the understanding of the benefits resulting from the use of IoT, especially those of personal or social nature. It should be made clear to intended users of IoT applications that IoT benefits go beyond business profitability and can contribute to helping people and society. IoT can offer benefits such as the improved life quality that can emanate from the application of IoT in several sectors such as healthcare, smart home, smart city and transportation. The IoT also brings ecological benefits stemming from the use of IoT for environment surveillance and protection. IoT systems for country borders or city surveillance can provide enhanced safety to citizens.

Thus, IoT success and adoption is sensitive to issues such as security, privacy and trust. The degree of the risk associated with these issues and its importance may vary across domains, as they depend on the nature of the data, the transactions and the parties involved in the IoT application. As IoT exists in diverse contexts with business and social implications, it is imperative for companies, organizations and governments to have an effective strategy that includes such socio-technical issues and take actions in order to ensure the mitigation of risks associated with the security and privacy aspects of IoT and promote the development of trust.

A regulatory and legal framework is also needed to be in place for the use of IoT applications in various sectors. Regulatory aspects and legal issues should be taken into account, regarding the use of the devices, data collection and use, and cross-border activities. This is particularly needed in mobile IoT because of the additional actions, constraints and risks resulting from the mobility of IoT nodes, such as in the case of aerial vehicles.

The economic facet of IoT is also fundamental for the success of any IoT-based business activity. Identifying the value proposition can be complex as the potentially interested parties may vary for each case and may have different needs and interests across domains. Pricing strategies and models adopted for the provision of the IoT-enabled product/service and how they can differentiate in various applications in diverse domains are also factors that call for new approaches combining technical and economic analysis. Pricing can be dynamic, adjusted in real-time, according to current conditions.

Revenue models and pricing policies should be carefully designed as part of any IoT-based business model, considering the increased and complicated management needs of data, devices and stakeholders. In particular, they have to take into account the potential social, commonwealth purpose of an IoT application, in sectors such as healthcare or environment protection. Profitability is undoubtedly a basic goal of any business model, and remains a top goal of IoT investments across industries. However, the pervasive and ubiquitous character of IoT offers value creation possibilities that extend business opportunities beyond the traditional economic goal of profit to serve communities and society. Profitability can still be achieved, through efficient pricing or the cost reduction resulting from the IoT solution, but it does not constitute the aim of the IoT application.

Several other issues of technical nature also have to be addressed before IoT can reach a broad applicability and commercialization. These could be summarized to: (i) Energy requirements of IoT have to be taken into account as the autonomy of devices, particularly of mobile unmanned vehicles (UAV, UGV, USV) is a critical success factor of any endeavor that involves them; (ii) Data requirements, including data exchange, storage and analytics. The unprecedented amount of data associated with the use of IoT creates new needs for the collection, transmission, storage and processing of data at both individual and organizational level. In addition, it raises issues that should be addressed such as data ownership and expiry; (iii) The need for interoperability of objects and systems is of paramount importance for the implementation of IoT ecosystems. The heterogeneity of devices with the diversity of technologies used which are associated with specific manufacturers generates severe impediments in data exchange and communication. The lack of standards and protocols create fragmented sets of IoT devices that are incompatible to co-operate as needed for an interconnected system.

5 Exploring the business potential of IoT: The case of RAWFIE

In this section, we present some indicative example scenarios for the use and applicability of IoT in selected domains. We focus on revealing the potential business models on top of the described scenarios. The scenarios are based on the RAWFIE project[1] that provides a platform for interconnecting multiple testbeds aiming at providing research facilities for mobile IoT devices, specifically unmanned vehicles (e.g., Unmanned Aerial Vehicles - UAVs, Unmanned Surface Vehicles - USVs, Unmanned Ground Vehicles - UGVs) for research experimentation in vehicular, aerial and maritime environments. The

[1] RAWFIE (Road-, Air-, and Water- based Future Internet Experimentation) is a project funded by the European Commission (Horizon H2020 programme) under the Future Internet Research Experimentation (FIRE+) initiative http://www.rawfie.eu

platform supports experimenters with smart tools for conducting and monitoring experiments in various domains of IoT, networking and sensing.

5.1 IoT in Environment Monitoring and Control

IoT, due to its autonomous nature, can satisfy the needs for environment monitoring and control where elaborate sensing, processing and possibly actuating are needed. Autonomous devices can be adopted to monitor specific phenomena and, when needed, to act or produce alerts. In this domain, we could identify the following application scenario:

Scenario 1 - Monitoring of Water Canals
In various countries, water canals are very significant as the quality of the provided water heavily affects human lives. Hence, there is the need of continuous monitoring the water and act when problems arise not only in the water quality but also in water supply. In this use case, an IoT platform could be used to mobilize resources that can collaborate for the purpose of monitoring of water canals and the collection of information that can be used for assessing the water quality and the endurance of the canal walls structure. The end user of this use case would be a water company, responsible for administering and monitoring multiple "islands" of water canals used for irrigation or drinking purposes. On a periodic or ad hoc basis the company wants to: (i) gather measurements regarding the concentration of grass and/or sediment on the bottom of water canals; (ii) detect cracks in the canal's wall structure; (iii) detect any potential problems with the quality of the water. In this way, the company can proceed with appropriate actions in case a problem is detected. Indeed, the collected information should be reported in company's premises in order to be analyzed (offline) and subsequent procedures for "cleaning" the canal are initiated if deemed necessary.

The business model behind this scenario involves not only the water company but also public authorities and citizens. Public authorities and citizens should be informed, immediately, for possible problems to apply response and mitigation plans. Apart from the direct impact in citizens' lives, there is also an economic impact. Water companies and public authorities could reduce the time required to identify potential problems as well as costs for applying any response plan. New investments could be adopted from public authorities and water companies related to more complex, however, efficient sensor platform that will be included in the IoT devices. These sensors will have the responsibility of recording various parameters related to the water quality. Through such an approach, a lattice of IoT devices could monitor the entire infrastructure with clear benefits for public authorities and citizens.

5.2 IoT in Safety and Security

Nowadays, safety and security issues are crucial for modern societies. IoT satisfies the needs of the security industry through the autonomous nature of IoT nodes and sensing and advanced on board processing needed to perform tasks like object detection and sensor information fusion. Critical areas / domains can easily be monitored without jeopardizing humans' lives as IoT nodes (especially, mobile devices) can be placed anywhere. In this aspect, we propose business scenarios for the surveillance of borders and the efficient coordination of dangerous phenomena identification.

Scenario 2 - Border Surveillance or Perimeter protection of large areas
In this use case, an IoT platform could be used to mobilize resources that can collaborate each other for the purpose of border, infrastructure or sensitive area monitoring and gather information that can be used for assessing a potential threat and take urgent action to protect the area or borders from invention or asymmetric threats. The potential environments of this scenario are land/sea borders or a camp/ infrastructure, environments that need constant monitoring with special focus on areas which are difficult to be reached by humans. The business model in this case involves a set of potential end users like: (i) the owners of critical infrastructures (e.g., energy production facilities, water treatment facilities); (ii) airports-

ports-central cargo railway stations; (iii) forest protection organizations; (iv) border security units. According to the scenario, security forces and commanders, which are located at an operational center, could have an overview of the monitored area through a platform (like RAWFIE's). Images, indications and generally information, coming from the stationary surveillance sensors (cameras, radars etc) which are deployed along the borders or the perimeter of a crucial infrastructure, are gathered and analyzed by the platform. On a periodic or ad hoc basis, the collected information could be checked for accuracy by using UxVs. In case of an alarm for a potential threat or intrusion detected by the security sensors (fire detector, acoustic sensor, motion sensors, CBNR sensor etc.) or cameras, automatically UxVs are deployed by the platform to collect more specific information. The collected information should be reported to the operational centre in order to be assessed by people in charge and decide the course of action that should be taken to face the threat. It becomes obvious that the economic impact is high as the critical infrastructure protection is of high importance for every country worldwide. A 'grid' of IoT devices that continuously monitor such facilities will become the necessary framework for prevention, identification and immediate response in potential problems.

Scenario 3 - Efficient Coordination for phenomena or mission coverage

This scenario deals with the efficient coordination of multiple mobile IoT devices for the purpose of covering certain phenomena (e.g., fire spreading in an area) or executing a certain sensing mission (e.g., mapping or scanning of an unknown area). The purpose is to explore various issues and strategies that can be adopted for intelligent coordination and control of multiple devices while minimizing resources consumption. Potential users of this scenario could be National Fire Brigades, Command and Control Centers (C&C), UxV manufacturers, public authorities, ports, airports, etc. A set of services could arise on top of this infrastructure ranging from the efficient navigation of IoT devices (e.g., when an event is identified by a device, other devices could reach the area to confirm it) to user-oriented interfaces. With the term user-oriented interfaces, we depict the GUIs adapted to each stakeholder's needs. For instance, the GUI required by the National Fire Brigade could differ when compared with the GUI required by the C&C of the local municipality or police. Usually, C&C require specific messages in standardized formats while firefighters may require user-friendly information (e.g., colors, data related to the spread of a fire).

5.3 IoT in Communication Infrastructure

First and foremost IoT can be used as a communication infrastructure. This can be deemed as a horizontal application of IoT technologies, contributing to other types of applications that are based on IoT technologies. In this direction, IoT is viewed in terms of a set of structural elements forming a new sophisticated infrastructure enabling advanced communication among various devices, by providing enhanced network connectivity and sensing services. Such a communication infrastructure can serve as a springboard for the development of innovative business models and applications that leverage the characteristics of IoT. Thus, IoT can have an auxiliary yet strong and essential role offering the technical basis needed for new and existing products and services. At the same time, apart from supporting others, IoT as an infrastructure can be a business model itself for a wide range of organizations in industry, academia and the public sector. IoT technology providers can benefit as business actors as the IoT functionality can be available in various domains in the form of experimentation platforms, integrated network environments and advanced technical facilities provision.

Scenario 4 – On demand deployable Internet facilities

The scenario tackles the rapidly expanding domain of on-demand deployable Internet facilities through UxVs. An illustrative example could be the provision of broadband connectivity to remote locations without such communication capabilities or to areas affected by phenomena/natural disasters like earthquakes, floods etc. where these moving Wi-Fi hotspots will provide Internet connectivity in an underdeveloped or semi-urban environment. Imagine a UAV (or swarm of UAVs) overflying the area. Each UAV will offer an access point like functionality to the local population (permanent residents, crisis management groups, etc.). The unmanned systems could form a multi-hop network in order to relay traffic to and from fixed infrastructure that has not been impacted. The same architecture could be based either on other types of UxV (e.g., a USV could provide connectivity to small islands), or on UAVs that have landed on suitable locations or even on their collaboration in mixed formations. In order to accomplish this difficult undertaking task such devices need to be extremely energy efficient (possibly solar-powered) and to operate for long without external intervention. Potential end user of this scenario can be an Internet Service Provider (ISP) or Search and Rescue (SAR) teams in case of emergency. ISPs can offer their services on top of the mobile IoT devices while SAR teams could 'secure' their communications in areas affected by a disaster.

Scenario 5 - Over the air re-programming
The scenario deals with network-assisted programmability of devices. Over the Air programming is a technique that is widely used in the mobile world for performing firmware or software updates mainly of cell phones. Extending this capability to the world of devices with strict real-time characteristics is quite a challenging task. A simple scenario involves the transmission and hot/cold installation of mission or operational related code from the ground control station (over-the-air (OTA) programming). Additionally, in a more generic aspect, re-programming could involve the application of software updates in numerous IoT devices and sensors placed in the field. The end users of this scenario could be software companies, IoT devices manufacturers or network providers. All of them through the envisioned framework could send their software to the devices keeping them up-to-date and securing a high QoS in their services. For instance, imagine a company that offers the operating system for a type of devices. The company identifies gaps in the provided operating system (e.g., a security gap) and wants to apply updates / patches in the entire set of devices. The over the air re-programming aspect of this IoT oriented setting will assist in the delivery and the application of the updates to all the devices.

6 Towards identifying mobile IoT business models

Following the described application scenarios and the proposed framework, we proceed to further examine RAWFIE from a business model perspective. RAWFIE platform supports experimenters with smart tools to remotely conduct and monitor experiments in the domains of IoT, networking and sensing. RAWFIE federation allows for multiple types of experimentation, including testing among different UxVs (e.g. UAVs) and UxV types (e.g. UAVs with UGVs) from different manufacturers and among different testbeds. The stakeholders can be the testbed providers, the unmanned vehicles/devices (UxVs) suppliers and the experimenters.

Business models can be created under the generic umbrella of offering (a) the available testbeds, (b) the devices and (c) the software tools, for experimentation across various domains to interested parties. These three assets can be offered either separately or in combination. Potential customers of such business models can be universities, research institutions, public organizations (police, army, fire brigade, local authorities, ecological bodies), and industries (UxV manufacturers, software developers, electricity/water companies). Revenue models can be subscriptions, license, or pay-per-use with charge per experiment or per testbed or based on the number and the type of devices used.

Another type of business model can emanate from the RAWFIE platform serving as a consolidator of testbeds and UxVs, an intermediary business entity which testbed providers and UxVs suppliers can join under various payment schemes. Intended RAWFIE customers-members can participate by paying a subscription or a commission based on their own revenue resulting from their use through the platform by RAWFIE customers. In this approach, testbed and device providers, who were previous RAWFIE stakeholders, become customers, extending RAWFIE business partnerships by adding new collaborations and new revenue channels. In this way, RAWFIE can be a mediator between infrastructure (testbed) and equipment (UxVs) providers and end user entities interested in using RAWFIE facilities. With such a business model, RAWFIE allows for a full implementation of Platform/Infrastructure-as-a-Service and Experimentation-as-a-service.

RAWFIE comes in a promising setting with vast opportunities thanks to the growth in UxV manufacturing, applications and sales and the diversity of domains that mobile IoT can be potentially applied to. RAWFIE's main strength is its pioneering characteristics, as it is an innovative, unique platform offering a federation of testbeds with mobile devices and providing interoperability of both testbeds and devices. On the other hand, RAWFIE is a new federation, with lack of experience and user/customer awareness and could be also be threatened by the development of competitive mobile IoT nodes platforms. Energy requirements of mobile devices, and, in particular, the idle time needed between experiments for device charging and maintenance are weaknesses that could also hinder the successful implementation of RAWFIE business models.

7 Conclusion

IoT technologies offer unprecedented opportunities to entrepreneurs and researchers for advancing their activities in novel paths towards a new environment that changes how we work and live. This paper approached IoT from a business perspective, contributing to our understanding of the IoT business value by highlighting the potential of IoT and the challenges for its realization. In this direction, it presented a proposed framework for the categorization and analysis of business models and their characteristics that can be used across application domains. The paper also showcased the applicability and business value of IoT through the description of specific cases of mobile IoT business models from the RAWFIE project. We believe that the framework in conjunction with the example cases can help both researchers and practitioners towards understanding IoT as a business enabler and identifying business models in various sectors, by taking into account several parameters that can positively or negatively affect IoT applicability.

We further suggested that in order to gain a complete understanding of the IoT potential and how it can be leveraged effectively, the IoT value should be examined with respect to technical as well as non-technical factors related to IoT. Our discussion focused on security, privacy and trust, economic aspects of IoT as well as other issues that should be taken into consideration. As IoT penetrates the modern world bringing radical changes at personal, business and society level, it calls for a socio-technical approach in research and practice.

The future of IoT appears to be very promising for industry or academia, in diverse sectors. Further research is needed to investigate more thoroughly the opportunities for exploiting IoT across domains, examining either how to augment current existing activities or how to enable new ones that have not yet been identified. Research should also study the challenges for the use and adoption of IoT and the ways they can be efficiently addressed. Further research efforts should particularly be directed towards finding effective solutions for overcoming the technical limitations of IoT. Having solved any general technical feasibility problems, any future work related to IoT should view how it can be applied within the personal, organizational or social context for which it is aimed. Because of its pervasive and ubiquitous nature, enabling its presence and involvement in practically every possible activity, IoT business value should be studied in conjunction with the social context within which it exists. In this vein, future research should investigate social aspects of IoT and how such aspects in turn influence the use of IoT in the new business ecosystem.

Acknowledgment

This project is funded by the European Commission (FIRE+ challenge, Horizon 2020) that aims to provide for research, technological development and demonstration under grant agreement no 645220 (RAWFIE).

References

Abdulah, P., Waseem, S., Bai, R., Mohsin, I. (2008). Development of New Water Quality Model Using Fuzzy Logic System for Malaysia. *Open Environmental Sciences*, 2, pp. 101-106.

Al-Sakran, H. O. (2015). Intelligent traffic information system based on integration of Internet of Things and Agent technology. *IJACSA*, vol. 6.

BI Intelligence (2016). The Internet of Everything. Report available at http://www.businessinsider.com/intelligence/bi-intelligence-iot-research-bundle

Bucherer, E., Uckelmann, D., "Business models for the internet of things," in Architecting the internet of things, pp. 253–277, Springer, 2011.

Chan, H. C. Y. (2015). Internet of Things Business Models. *Journal of Service Science and Management*, 8, pp. 552-568.

Chepuru, A. & Rao, K. V. (2015). A study on security of IoT in Intelligent Transport Systems Applications. *IJARCSEE*, vol 5.

Erol-Kantarci, M., Mouftah, H. T. (2010). Wireless sensor networks for domestic energy management in smart grids. *Proceedings of the 25th Biennial Symposium on Communications (QBSC)*, pp. 63–66.

Fleisch, E., Weinberger, M., Wortmann, F. (2014). Business Models and the Internet of Things. *White Paper*, Bosch Internet of Things & Services Lab.

Gao, J., Xiao, Y., Liu, J., Liang, W., Chen, C. (2012). A survey of communication/networking in smart grids. *Future Generation Computer Systems*, vol. 28(2), pp. 391–404.

Gartner (2017). Gartner Says By 2020, More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things, available at http://www.gartner.com/newsroom/id/3185623

Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton, N., Razafindralambo, T. (2011). A survey on facilities for experimental Internet of Things research. *IEEE Communications Magazine*, vol. 49, pp. 58–67.

Gouveia, C., Fonseca, A. (2008). New Approaches to Environmental Monitoring: the Use of ICT to Explore Volunteered Geographic Information. *GoeJournal*, 72, pp. 185-197.

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Elsevier Future Generation Computer Systems*, vol. 29, pp. 1645-1660.

Hardas, B. M., Asutkar, G. M., Kulat, K. D. (2008). Environmental Monitoring Using Wireless Sensors: A Simulation Approach. *Proceedings of the 1st International Conference on Emerging Trends in Engineering and Technology*, pp. 255-257.

Hatzikos, E., Bassiliades, N., Asmanis, L., Vlahavas, I. (2007). Monitoring Water Quality through a Telematic Sensor Network and a Fuzzy Expert System. *Expert Systems*, 24(3), Blackwell, pp. 143-161.

Katiyar, V., Kumar, P. & Chand, N. (2011). An Intelligent Transportation System Architecture using Wireless Sensor Network. *International Journal Computer Applications*, vol. 14.

Kolomvatsos, K., Anagnostopoulos, C., Hadjiefthymiades, S. (2015a). An Efficient Environmental Monitoring System adopting Data Fusion, Prediction and Fuzzy Logic. *Proceedings of the 6th International Conference on Information, Intelligence, Systems and Applications*, Corfu, Greece.

Kolomvatsos, K., Anagnostopoulos, C., Hadjiefthymiades, S. (2015b). Intelligent Contextual Data Stream Monitoring. *Proceedings of the 8th International Conference on Pervasive Technologies Related to*

Assistive Environments, Corfu, Greece.

Li, X., Lu, R., Liang, X., Shen, X., Chen, J., Lin, X. (2011). Smart community: an Internet of Things application. *IEEE Communications Magazine*, vol. 49, pp. 68–75.

Martin C. (2015). The Top 5 IoT Success for Media & Entertainment Companies. Commentary, available at https://www.mediapost.com/publications/article/254890/the-top-5-iot-success-factors-for-media-entertai.html.

Newman, P. (2017). The Internet of Things 2017 Report: How the IoT is Improving Lilves to Transform the World. Business Insider, 2017, available at http://www.businessinsider.com/the-internet-of-things-2017-report-2017-1.

Oka, D. K., Furue, T., Langenhop, L., Nishimura, T. (2014). Survey of Vehicle IoT Bluetooth Devices. *Proceedings of the 7th International Conference on Service-Oriented Computing and Applications*, Matsue, Japan.

Osterrwalder, A. and Pigneur, Y. (2010). Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers. Textbook, Wiley.

Papert, M. and Pflaum, A. (2017). Development of an Ecosystem Model for the Realization of Internet of Things (IoT) Services in Supply Chain Management, *Electronic Markets*, 2017, vol. 27, issue 2, No 9, 175-189.

Pedrasa, M. A., Spooner, T., MacGill, I. F. (2010). Coordinated scheduling of residential distributed energy resources to optimize smart home energy services, *IEEE Transactions on Smart Grid*, vol. 1(2), pp. 134–143.

Srini, P. (2016). 5 Critical Success Factors – IoT Platform Adoption. Article available at http://www.netobjex.com/5-critical-success-factors-iot-platform-adoption/.

Swanepoel, L. (2016). Key Success Factors for an Enterprise IoT Strategy. Articles available at http://www.itnewsafrica.com/2016/03/key-success-factors-for-an-enterprise-iot-strategy/.

Valarmathi, M. L., Sumathi, L., Deepika, G. (2016). A Survey on Node Discovery in Mobile Internet of Things (IoT) Scenarios. *Proceedings of the 3rd International Conference on Advanced Computing and Communication Systems*, Coimbatore, India.

Wang, N., Wu, W. (2011). The Architecture Analysis of Internet of Things. Proceedings of the 5*th Computer and Computing Technologies in Agriculture (CCTA), Beijing, China.*

Westerlund, M., Leminen, S., and Rajahonka, M. (2014). Designing Business Models for the Internet of Things. *Technology Innovation Management Review*, 4, pp. 5-14.

Wilhite, J. and Mehraban, S. (2015). Critical Factors for Successful Internet of Things Deployment. Article available at https://www.automationworld.com/article/topics/industrial-internet-things/critical-factors-successful-internet-things-deployment.

Xiao, L. (2011). Internet of Things: a New Application for Intelligent Traffic Monitoring System. *Journal of Networks*, vol 6(6), pp. 887-894.

Zhang, Y. and Wen, J. (2016). The IoT electric business model: Using blockchain technology for the internet of things, *Peer-to-Peer Networking and Applications*, 10, 983-994.