# Internet of Things: A systematic review of the business literature from the user and organisational perspectives

***Abstract***

The Internet of Things is a new technological paradigm that aims to connect anything and anyone at any time and any place, giving rise to innovative new applications and services. In doing so, it offers a number of opportunities and challenges that users and organisations need to tackle. In this paper we systematically review the business literature related to the Internet of Things and provide a critical account of the latest state of play. More specifically, we adopt two perspectives: that of the user and that of the organisation. After outlining the methodological approach adopted, we consider the definitions of the Internet of Things. Then, in turn, we discuss the relevant business literature from each perspective. The paper concludes with a synthesis of the emerging themes and potential avenues for future research.

**Keywords**: Internet of Things, systematic literature review, business perspective, users, organisations

# Internet of Things: A systematic review of the business literature from the user and organisational perspectives

## 1 Introduction

The Internet of Things (IoT) promises a new technological paradigm, by connecting anything and anyone at any time and any place, using any path/network and any service [1-4]. The IoT vision is that of a *"smart world"* which is equipped with sensing technologies and smart components. The IoT features Web 3.0, which involves users much more deeply than its predecessor, Web 2.0, as they and their immediate physical environment are more heavily involved with the technology in ways that go far beyond content creation and sharing [5]. Not surprisingly, such a bold vision has captured the imagination and attention of both academics and practitioners, as the IoT could underpin innovative services and applications. The IoT is expected to have a significant impact on individuals, businesses, and policy as societal and business models will be challenged, and new services introduced [6, 7]. On the other hand, the IoT is not without its challenges and caveats. For instance, the pervasive nature of the IoT and the amount of data generated are likely to involve concerns about the invasion of privacy in an all-connected world.

Much work has been carried out over the past few years on projects related to the IoT. Among the 11 significant concepts depicting the future of information infrastructures and technologies (e.g. semantic web, ubiquitous computing, etc.), the number of publications related to the IoT stands out, as it has increased in recent years [8]. Given the wide scope of the IoT, it is important to make sense of the current state of play and inform the future research agenda accordingly. To our knowledge only a limited number of reviews have been published to date, but none of them have examined the business perspective. Atzori et al. published a review paper in 2010 that presents the visions and concepts including a classification and introduction of technologies enabling IoT, a framework of IoT relevant applications, and proposing potential avenues for further research [9]. Following a similar approach, Li et al. [10] provided an integrated view of the IoT, discussed the IoT service-oriented architecture, enabling technologies and applications, addressed the technical challenges, standardisation activities, security and privacy problems, innovation in IoT environment, and IoT development strategies in various regions as the main challenges for future research. Yan et al. [11] conducted a co-word analysis, finding that the most prominent keywords associated with the IoT are wireless sensor networks (WSN), radio frequency identification devices (RFID), and security. The frequency analysis of Mishra et al. [12] produced a similar finding, i.e. that RFID was the most frequently occurring keyword, while WSN and security ranked second and third. These three keywords and the clusters they represented represented over 80% of the IoT publications [11]. Hence, the enabling technologies and security issues of the IoT were the most covered research topics up to 2014. Lastly, Mehmood et al. [13] studied the centrality values ranked by country of a social network analysis of international co-authors and co-institutions and showed that China occupied the largest number of publications co-authored with other nations, followed by

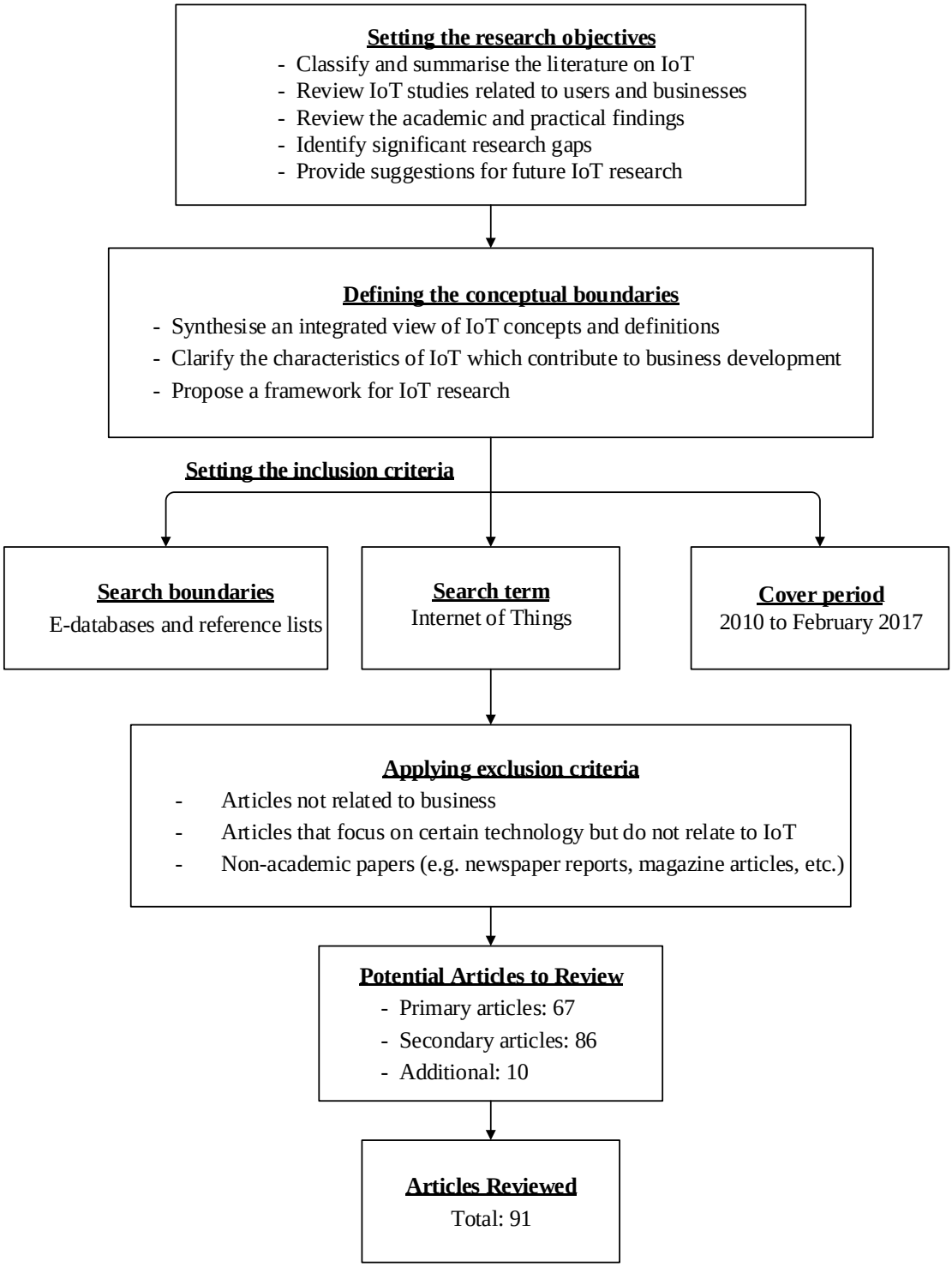
the U.S., Spain, and the U.K. Among the five review papers identified, three of them [11-13] conducted quantitative research that analysed the high-frequency keywords, highlighted the top cited authors, most effective journals, institutions and countries, and mapped the IoT to clusters. The other two studies [9, 10] qualitatively reviewed IoT related studies and identified emerging themes in this field, mainly focusing on the enabling technologies, applications, privacy and security issues, and open issues for future studies. Given that IoT technologies and services are steadily progressing technically and have reached mainstream markets, it is high time that the literature was also examined from a business angle. There is also a need to address a gap in the business related IoT literature, as none of the reviews so far has provided an analysis of IoT publications from the business perspective. In doing so, and by considering the business and innovation aspects of the IoT, we aim to tackle one of the open research issues identified by Li et al.[10]. In this paper we address the above-mentioned gaps by systematically reviewing the IoT literature published in recent years. Specifically, the objective of this paper is to identify and critically synthesise published work related to the IoT from the user and the organisational perspectives. It also aims to identify research gaps and propose new research avenues. The objectives set are achieved by first identifying and filtering relevant papers, then outlining their key attributes and finally by critically reviewing them under the emerging themes.

The following section outlines the methodology adopted for the systematic literature review. The review then focuses on the definition of IoT and its main charactiristics. The paper then presents the relevant literature on the user and organisational pespectives before concluding by proposing a number of future research avenues.

## 2 Methodology

In this paper we follow a systematic approach to reviewing the relevant literature following a number of steps, such as planning the review, selecting and reviewing the papers, synthesising the results, and reporting the findings [14]. The literature review process started with a database search, as shown in **Error! Reference source not found.**. We first searched databases for papers with appropriate selection criteria, then ranked and grouped them for review. We selected three electronic databases (i.e. Scopus, Ebsco, and Web of Science) which offered excellent coverage of the topics under study. Our search strategy revolved around the term *"Internet of Things"*. Using advanced search criteria, we restricted the source type to English full-text review papers, journal articles, and articles in press. Given that we were interested in the business side of the IoT, the academic discipline was restricted to the social sciences, arts and humanities, business management and accounting, psychology, as well as multidisciplinary areas. We downloaded information about 612 articles from Scopus, 115 articles from Ebsco, and 108 papers from Web of Science (total 835) that were available by February 2017. After identifying duplicates among the three sets, our list of papers included 772 papers. The information about the search results from the e-databases was organised so that it could be evaluated by the three authors independently. This made it possible to confirm the relevance of the selected papers and increase reliability [15].

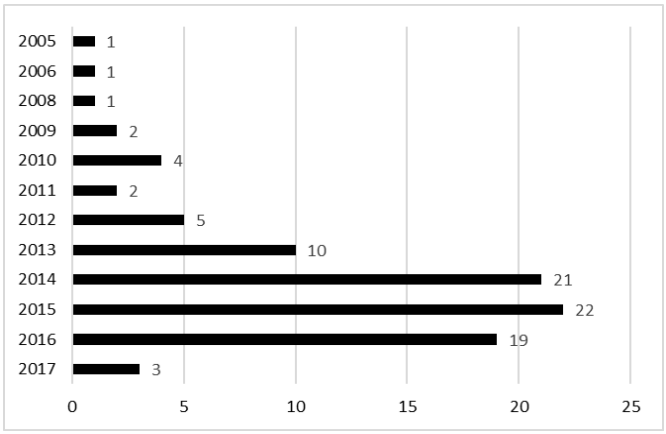
**Figure 1: Summary of the literature selection process**




The researchers reviewed the title, keywords and abstracts of the papers to decide whether they should be included in the review [15]. Firstly, given the objectives of this review, papers that were not directly relevant to either the user or organisational perspectives of IoT were excluded. Secondly, the authors excluded non-academic papers such as newspaper or magazine reports, as well as presentations or interview transcripts. The assessment then considered the rationale, credibility, and robustness of the research design [14]. We evaluated each paper by

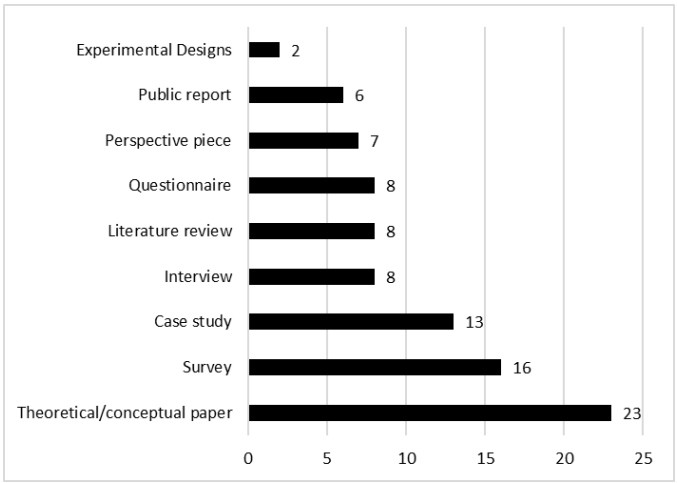
allocating a weighted relevance score (min 0 to a max 4), based on each researcher's selection and the times that a paper appeared in the databases. In turn, based on the scores, we clustered the papers into two main groups, namely those with the highest score (67 papers scored 3.33-4.00, which suggested that all three researchers considered them to be highly relevant and/or they featured in more than one database) and those that followed closely, but still had a distinct score gap compared to the first group (86 papers; scored 2.33-3.00). We then evaluated the final list to ensure that it was approved by all the researchers. After this confirmation we downloaded all the papers, excluding 5 articles that were not available. In addition, by reviewing the reference lists of the papers, 10 articles that had not been covered by the selected databases were added to the review list as they were cited several times. Among these 156 papers, only five papers were published before 2010 (Figure 2). The majority of the cited papers were published in 2014, 2015 and 2016.

**Figure 2:Year of publication**



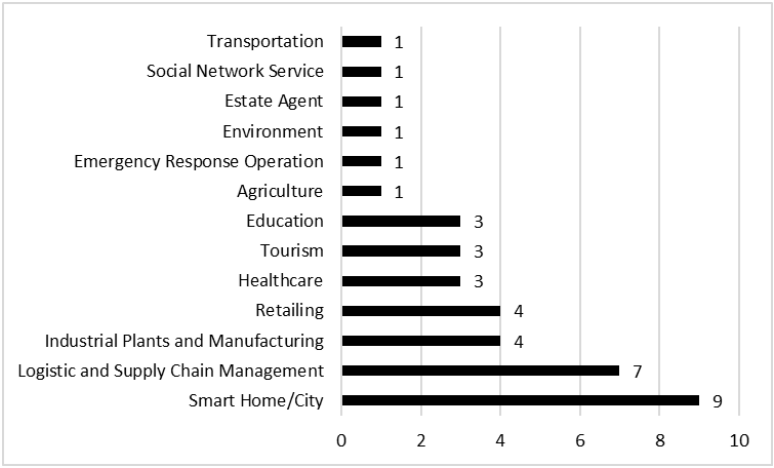

We reviewed 91 papers in total (Figure 3). Among these there were 23 theoretical/conceptual papers, 16 papers using surveys, 13 case studies, 8 papers based on interviews, 8 literature reviews (IoT or more broadly focused), 8 using questionnaires, 7 papers that were written from the author's perspective, and 6 public reports.

**Figure 3: Research methods adopted by the reviewed papers**



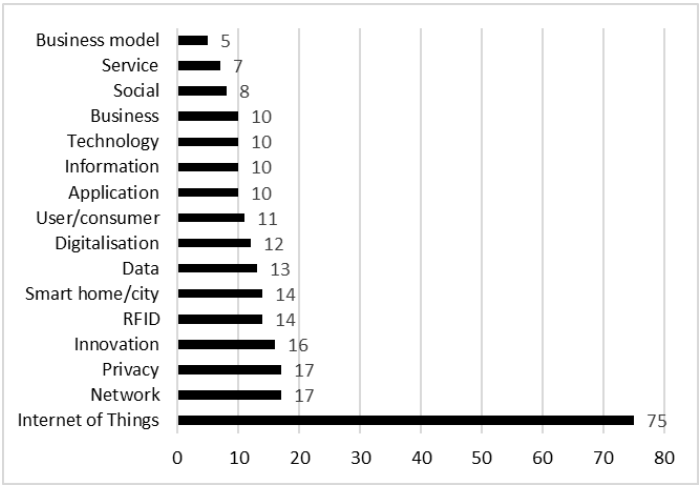
39 out of these 91 papers contextualised their studies in specific business sectors (Figure 4). The most attention-gaining business aspects of the reviewed papers were those related to smart homes/cities, followed by those in the area of logistics and supply chain management, industrial plants and manufacturing, retailing, and healthcare.

**Figure 4: Business sectors considered by the papers reviewed**




The keywords featuring in the reviewed papers were semantically clustered and the frequencies of the clusters calculated (Figure 5). Not surprisingly, IoT was the most frequent cluster. The keyword analysis offers evidence that the business literature closely follows established themes identified in earlier reviews.

**Figure 5: Frequency of keywords found in the papers reviewed**




## 3 IoT Definitions and Characteristics

We embarked on our analysis by considering the primary set of data to identify definitions of the IoT. The analysis identified three popular definitions. The first one was by Atzori et al. [9], who stated that IoT is a result of the convergence of three visions, namely *"things-oriented"*,

*"internet-oriented"*, and *"semantic-oriented"* visions. They first introduced the IoT semantically as *"a world-wide network of interconnected objects"*. They approached the IoT from the viewpoint of the *"pervasive presence"* of uniquely addressed objects around people that are able to interact with the other objects and react to the physical environment and thus reach common goals [9]. The second definition, put forward by ITU [16, 17], suggested that the IoT is every object of the physical or virtual world which *"is capable of being identified and integrated into communication networks"*. Finally, one of the most representative definitions (and also the working definition for this review) was proposed by the European Commission [1], conceptualising the IoT as a dynamic global network infrastructure that will be integrated into and act as an extension of the future internet, in which various *"things"* have unique identities, physical attributes, virtual personalities, and intelligent interfaces. Put differently, *"the Internet of Things will allow people and things to be connected any time, any place, with anything and anyone, ideally using any path/network and any service"* [1]. The term "*things*" acts as a new dimension of the extension of current existing human and application interaction, thus enabling people and objects to be connected, exchanging real time information via any path [1-4].

The identified definitions have a great deal of overlap in that they share a few common characteristics, such as the dynamic network, the global infrastructure, the interconnection and interaction between humans and things, the pervasive presence of connected uniquely identified objects, and the spanning of time, space, and paths. The purpose of the IoT is to make possible the efficient sharing of real-time information among autonomous networked actors [18]. The IoT refers to the pervasive presence of billions of intelligent communicating objects that are connected in an Internet-like structure which can be considered as part of the future Internet, cities and the world itself, which will be overlaid with smart objects that can sense and react (a smart world) [6, 7, 19, 20]. Objects in a future smart world will be uniquely identified, accessed and verified over the Internet. These items will have a virtual representation or digital shadow that will be stored in cyberspace, enabling communication and interaction between humans and objects or machine to machine [21-27]. The objects can communicate with computers without human involvement, making the Internet more immersive and pervasive as a communication paradigm [28-30]. Based on an objects-oriented viewpoint, the IoT is envisioned as a ubiquitous global network of connections of machines and devices that are capable of interacting and interconnecting with each other [31-33]. This enhances an increasingly connected world that achieves the goal of intelligently identifying, locating, tracking, monitoring, and managing things in real-time [34-36]. The interconnected objects form a network that can not only harvest information from the environment, but also interact with the physical world. Such interactions merge the physical and digital world and extend the benefits of the Internet to the physical world, such as constant connectivity, remote control, and data sharing [6, 32, 37, 38]. Similarly, the IoT describes an emerging global information service infrastructure that extends the Internet into the physical world, fusing the borders between physical entities and virtual components [22, 39, 40]. The IoT and the realisation of the digital and smart network requires the use and integration of almost all information technologies in implementing the process of information acquisition, transmission, and application [23, 41, 42]. The social, environmental, and user context-aware objects will be able to cooperate with other things and communicate with their

physical and virtual surroundings to execute tasks and meet personal needs in a way that does not incur the same limitations as people [9, 43-45]. The intelligence enhanced by IoT global architecture facilitates the exchange of goods and services, the interaction between smart objects creates the availability of services, and the emergence of the IoT concept brings opportunities for service innovations [4, 40, 46]. Social systems are on the way towards full connectivity, creating a society where every device is connected, which is why the IoT has been considered to be a technological revolution and a process of social shift [47-50]. As the world is becoming data-rich, the supersets of connecting devices and associated processes will lead to sharing and exposing more information and keeping fewer secrets, which leads to considerations of privacy protection and security issues [51, 52].

To better understand and appreciate the challenges and opportunities that such a complex vision entails, in the next two sections we proceed to review the business-related literature from the user and organisational perspectives.

## 4 User Perspective

In studies considering users in the context of the IoT, the most common foci are on customers' preferences of characteristics related to product design, users' acceptance and intention to purchase novel technologies, as well considerations of safety and privacy issues. We discuss these in turn in the following sections.

### *4.1 Users' Perception and Product Design*

As the IoT leads social shifts in human life by offering products with various functions and target scope, the characteristics that have a significant impact on consumer purchase intention and good-practice principles in product design are discussed in this section. Chang et al. [31] found that purchase intentions are determined by six characteristics and are mediated by customer experiences. The characteristics are: (a) IoT Connectivity: *"the degree to which things are interconnected"*; (b) IoT Interactivity: the customers' feeling that occurs when information communication is bidirectional and response is timely; (c) IoT Telepresence: the subjective feelings of customers about *"the extent to which media represent the physical and social environment"*; (d) IoT Intelligence: intricate and accurate recognition functions, correct thinking and judgment capabilities; (e) IoT Convenience: *"the degree to which consumers save time and effort in the process of planning, purchasing, and using a product"*; (f) IoT Security: damage avoidance when it comes to any vulnerable and valuable assets. The mediator between IoT characteristics and purchase intentions is the experience, which refers to the customers' overall impression of external marketing incentives that can have a profound impact on their behaviour. The experience can be categorised into two types: i) the functional experience, which refers to objective cognition, and ii) the emotional experience, which represents the subjective emotions of IoT consumers. All product characteristics were found to have a positive impact on consumer purchase intention via functional and/or emotional experience [31]. Findings suggest that IoT product design, promotion, and management should focus on improving customer experience [31].

The study by Rau et al. [20] presented a design of an interactive IoT application on a mobile platform based on the social web of things (SWoT) concept, which made it possible for the users to interact with the IoT in the same way they interact with social network services. It revealed three additional characteristics related to IoT application design that may affect users' choices, namely effectiveness and consistency, flexibility, and privacy. When designing interaction systems, effectiveness and consistency are always important considerations, since users prefer applications that are able to improve the convenience of their life by clearly and simply solving the decision-making problems [20, 53]. Then, as different customers hold different values and choice preferences, the functions and features have to be flexible and tailored to their preferences (these can vary based on demographics, such as age and education). Privacy, information authorisation, and customers' values should also be considered by product developers (discussed in more detail below), as users need to control their private and personal information and protect it from other people or entities [20]. Privacy of information and authorisation of content usage are critical issues because most users regard IoT applications as private tools [20]. The following seven ground principles could help provide a working design framework for building security and privacy into IoT applications: (a) proactive and preventative protection of privacy; (b) default instead of optional privacy protection; (c) embedded rather than add-on privacy protection in the product or service; (d) functionality of the product not obstructed by privacy; (e) security applied to the entire system; (f) accountability and trust supported by visible and transparent privacy procedures; (g) respecting and empowering user to manage their data [52].

### *4.2 Technology Acceptance*

Given the technological nature of IoT services, the user's acceptance of the underlying technologies is very important when it comes to adopting a service. *"For companies, lack of user acceptance of new technology has long been a painful obstacle in the technological innovation process"*[54]. When it comes to IoT acceptance, three models have been widely referred to and applied, namely the unified theory of acceptance and use of technology (UTAUT) [55], the technology acceptance model (TAM) [53, 56], and the task-technology fit model (TTF) [18]. These models performed well in explaining the determinants of IoT adoption by users.

Acceptance studies have typically adopted the users' intention and behaviour towards IoT technologies as dependent variables. The most commonly considered determinants are perceived usefulness and perceived ease of use, first proposed by TAM [53, 56]. For instance, a study of Chinese users' adoption of mobile smart homes by Bao et al. [56] shows that the users are likely to adopt the service if they think that it is useful, while perceived usefulness acts as a mediator between the perceived ease of use and behavioural intentions. Another study on the acceptance of IoT technologies found that fun and pleasure are additional characteristics which should be incorporated in IoT functions [53]. Therefore, in addition to usefulness and ease-of-use, fun and enjoyment are also expected to be obtained in IoT functions [53]. In addition, emerging innovative technologies usually come with risks, which will also significantly influence consumers' intention and behaviour [53]. Beyond privacy and security issues, the characteristics of IoT technologies, intangibility, and a high level of IT involvement may lead to a higher level of perceived uncertainty and risk for the users [53]. Both of these

studies based on TAM concluded that social influence, which represents the users' value and belief associated with societal influences (the degree to which an individual perceives that important others believe he or she should use the technology [55]) is one of the most important factors in IoT service and technology adoption [53, 56]. Social influence is considered to play a particularly important role in an early stage of technology diffusion since most users lack reliable information about the new product or service [53]. Early adopters should be identified as theycould help facilitate the diffusion of IoT services [53]. Chong et al. [55] studied RFID adoption in the healthcare supply chain by adapting the UTAUT model to incorporate individuals' *"Big-5"* personality traits (i.e. neuroticism, conscientiousness, openness, agreeableness, and extraversion). Results show that performance expectancy is the strongest, while effort expectancy is the least important predictor among the UTAUT variables [55]. In addition to the TAM and UTAUT models, Yang et al. [18] published a study using the task-technology fit (TTF) model. Task-technology fit refers to the degree to which IoT technology assists an individual in performing their portfolio of tasks, and correspondence between task requirements, individual abilities, and the functionality of the technology [18]. This study conceptualised this factor as one comprising four dimensions (i.e. resource and personal accountability, situation assessment, resource allocation, and multi-organisational coordination) in the context of emergency response operations [18]. Emergency response operations enhanced by these four perspectives are able to add strategic value to information sharing, retrieving, and explanation, which was contributed to by IoT technology characteristics [18].

In addition to the above-mentioned widely accepted models, Hsu and Lin [57] developed a conceptual framework to understand the motivations of continued use of IoT services by investigating network externalities and information privacy factors. Information privacy protection is of high concern for users. Data collected by the service providers may be beyond the users' control, be accessed and used without authorisation, or may be erroneous. Based on these concerns, four facets of concerns about information privacy are summarised as: collection, unauthorized secondary use, improper access, and errors. Results show that the privacy concerns have less effect on users' continued intention to use compared with the perceived benefits, i.e. direct and indirect network externalities [57]. The perceived compatibility and complementarity that indicate indirect network externalities significantly influence the continued use intention [57]. This implies that users are more willing to adopt and use the IoT services when they are perceived to be compatible with the users' values and beliefs. Also, the perceived benefits can be derived from complementary products and services [57]. In the retail industry enabled by the IoT technologies, the continuance intention of customers is also influenced by perceived value co-creation, which is determined by consumer experience attributes, i.e. perceived ease of use, superior functionality, presence, and aesthetic appeal [58]. Accordingly, with the aim of enhancing perceived value co-creation for customers, retail stores should ensure that the adopted IoT technologies a) are user-friendly, thus reducing customers' emotions of frustration and discomfort; b) are able to improve the effectiveness in the shopping process; c) satisfy customers' senses and immersion [58].

The user's acceptance and adoption intention studies have provided several implications for businesses. Bao et al.'s [56] research confirmed that the smart home is a pivotal initiative of the smart city concept which drives the development of cities and attracts business and

investment opportunities. In this case, the determinants of users' adoption intention play a necessary role in investigating the implementation of smart cities [56]. Given that social influence has been found to be an essential adoption factor, business strategies could be adjusted accordingly, for example, offering financial incentives to users who recommend IoT products to others in order to encourage the promotion and diffusion of IoT [53, 56]. Also, promotions such as those demonstrating the product or concept to users and letting customers experience them could help to increase the users' perceived ease of use and usefulness [56]. During the designing process, effectiveness and efficiency should be thoroughly examined to increase the perceived value and benefits for users [53, 57, 59]. Potential users of IoT have both extrinsic and intrinsic motivation, they also expect the fun and enjoyment brought by IoT products, so it is suggested that entertainment functions be provided by practitioners [53]. As far as privacy is concerned, a clear contract between users and providers that states the liability and privacy-preserving mechanisms would be helpful [57]. It is crucial for service providers to motivate user adoption by ensuring that the service fits well with users' values, which contributes to reducing the perceived risk of adoption [57]. The compatibility between different devices and services is also essential in companies' long term strategy, thus standardisation of interactions among devices and services needs to be developed to avoid hindering diffusion [56].

### *4.3 Privacy Issues*

If the IoT is to bring about significant benefits, managing user expectations towards privacy will help build their trust, confidence, and acceptance of IoT services, and consequently make it possible to reach their full potential [33, 51, 60]. On an individual level, privacy is regarded as a double-edged sword: users consider privacy controls as a protection of their personal information, but the risk of privacy invasion could be a barrier to IoT acceptance [27]. In line with the information privacy concerns discussed in the previous section, the four key user concerns are [61]: (a) surveillance without the individual's consent: sensors and applications might be used to track people's movement and behaviour and create multiple large data sets, hence encouraging surveillance; (b) uncontrolled data generation and use: in an interconnected web of applications and sensors, the process of diffusion of the collected data is almost uncontrollable; (c) inadequate authentication and preservation of anonymity: current centralised service authentication does not provide security in controlling access, and the automatic identification between services leads to new risks; (d) security risks of collected information: IoT can potentially collect and transfer a large volume of information using multiple collaborative devices, thus becoming a potential risk to security.

These key concerns reveal two main challenges in privacy protection of the IoT: the control of data generation and the security of information. The first challenge is due to the pervasive nature of the IoT and the dynamic change of contexts. One of the key facets of IoT service development is the improvement in consumers' quality of experience, which needs to enhance the connectivity in the relationships between humans and things [62]. Also, changes in time, space, culture, and the need for interaction between various systems drive dynamic contexts with different privacy policies, resulting in challenges for IoT offerings in adjusting to dynamic requirements [7]. Therefore, privacy development must be assessed in specific contexts [40]. This challenge could be addressed by legislation. An important principle in cyber privacy is

applying privacy protection based on the context in question. For example, people expect a different level of privacy in activities at home and in public, thus the level of protection varies accordingly [50]. It may be feasible to customise and differentiate privacy and security policy to fulfil individual needs while a contextual information relevance model of privacy is proposed respecting the unique needs [27]. Additionally, legislation issues toward privacy protection are widely recognised and discussed, especially in the United States, the European Union and China [9, 40]. The discussions focus on the legal challenges, questioning the need for laws to govern the changes brought about by the IoT, the sufficiency of existing law, what kind of law is required, and the related implementation time frame [40]. Even though there is no consensus on what is essential for privacy law and how it can be appropriately addressed, privacy protection policy should guarantee a number of key principles, such as data anonymization, e.g. the position and movements of people collected by tracking systems should not be linkable to the users' identities, but only be considered as aggregate users; leaks of information and privacy breaches should be notified to users; collected data should be processed for the sole purpose of delivering services; transparency of data collection and accountability of data collectors should be improved [9, 40, 63-65]. The second challenge arises from the massive information collection in the IoT. It will become almost impossible for an individual to avoid being monitored and recorded by sensors in public spaces. Once the information is generated, it might be retained indefinitely and it will be impossible to control the disclosure at a personal level [9, 63]. When designing IoT applications, data generation, collection, mining, transmission, and interpretation are central considerations. A major improvement in the amount of personal data (e.g. location and movements, health conditions, finance conditions, etc.) will be recorded, thus information protection is vital since privacy protection directly influences customer experience and trust in IoT offerings [33, 52]. As far as the need to delete user information on demand is concerned, a solution can be provided by service providers' "forget-me" functions [9].

## 5 Organisational Perspective

This section reviews the emerging IoT applications and functions, offering insights as to their potential impact on organisations. After considering potential business applications, this section discusses the issues of value creation, strategy, innovation, design and security among other things.

### *5.1 IoT Business Applications*

Most of the early IoT products have been developed by simply equipping existing objects with sensors or tags, thus facilitating the collection, processing and management of information. Even though only a small number of applications and services is currently available, it is very challenging to predict the full potential impact of IoT due to the pervasive nature and the rapid improvement of enabling technologies which facilitate different activities and satisfy the diverse needs of users [6, 9]. Table 1 summarises IoT applications in 14 service domains, by categorising them into four types according to their target and scope of adoption. Similarly, an analytic hierarchy process (AHP) model has been proposed to assess and compare the viability and prospect of a number of IoT applications oriented to the customer, business, and the public

[54]. The model includes three main criteria and 11 sub-criteria in a hierarchy: technological prospects (i.e. technical practicality, technical reliability, cost efficiency, and standardisation), market potential (i.e. market demand, user acceptance, business model, and ecosystem building), and regulatory environment (i.e. industrial regulation, consumer protection, and government support). Among these, the market potential weighs most and the four sub-criteria ranked the top 4. By applying the AHP model, researchers found that IoT logistics is the most promising IoT application, followed by IoT healthcare and IoT energy management respectively [54].

**Table 1: IoT Services and Applications**

| Application Level | Service Domains | Descriptions and Functions |
|---|---|---|
| Infrastructural Level | Smart Environment | Concentrates on environment monitoring and protection. Wireless sensors measure environmental indicators (e.g. pollution, water quality, temperature, humidity) and proceed to the information platform, which triggers alerts and actions [36, 46]. |
| | Smart City | City equipped with various IoT devices and systems, aimed at monitoring, analysing and sharing information and coordination within a city system [6, 36]. Helps governments and other stakeholders to improve city planning [9, 36]. |
| | Smart Energy | Enhances users' awareness of usage control by services such as smart power grid, smart meter, and remote meter reading [6, 36, 46]. |
| | Smart Tourism | A networked system of tourism destination including industries, services, and visitors in emerging forms of technological infrastructure that facilitates data transformation into value propositions, supports cooperation, knowledge sharing, and open innovation [45, 66]. The tourism supply chain management can be enhanced with geospatial data enabled by IoT technologies, thus improving sustainability in tourism destinations [67]. |
| Organisational Level | Smart Logistics and Supply Chain Management | Contributes to shortening process and reaction period by obtaining real-time information monitoring for enterprises [9, 36]. It also facilitates resource utilisation, quality management, safety and traceability [46]. |
| | Smart Agriculture | Conservation status monitoring and transportation management, facilitating inventory control, distribution management, and logistics of perishable agricultural products [6, 9, 36, 46]. |
| | Industrial Plants and Manufacturing | Optimising the production process in digitalised industrial plants by deployment of identification tags and interaction with the intelligent network [9, 46]. This enhances process controlling and tracking, industrial environment monitoring, product lifecycle monitoring (PLM), safety and security, energy saving, and pollution control in production processes [36]. |
| Individual Level | Smart Home | Enabled by connecting items and devices at home which form a wireless sensor network to enhance applications in security, intelligent indoor environment control, household appliance control, smart metering and energy saving, thus creating a smart and comfortable private space [9, 36, 46, 68]. The devices, data processing hubs, the cloud, and third party applications constitute a general smart home management system/platform that clarifies the specific tasks and requirements for smart homes [68, 69]. |

| | | |
|---|---|---|
| | Entertainment and Gaming | Intelligent system that can adjust the game activity and difficulty level with the excitement and energy levels of the gamer by sensing the parameters of the players [9]. |
| | Social Networking | Smart devices automatically update information about the users' real-time location, mutual friends' meeting, and attendance at events or social web pages, which reduces effort [9, 46]. |
| | Smart Safety | Protects personal and community property by reading identification tags to alert owners or security guards when an item is moved without authorisation and recording location information of the movement to help users track items [9, 46]. Ensures safety in both public and private spaces by controlling the accessibility of critical information which requires personal identification, monitoring dangerous cargo, food and water safety, alerting and responding to emergencies in communal facilities [36, 46]. |
| All-Inclusive Level | Smart Transportation | Auto-control and intelligent regulation of connected vehicles effectively reduces time spent on commuting and energy consumption. Provides real-time road status, navigation, and assisted driving to the users and improves road safety and transportation efficiency [6, 9, 36, 46]. |
| | Medical and Healthcare | Devices provide opportunities for remote and participatory medical services by monitoring personal health conditions and alerting for potential disease [6, 36, 46, 70]. Patient and medical resource management systems in hospitals and pharmacies, contribute to more efficient and effective treatments [6, 9, 36, 46]. |
| | Education | Applications facilitate learning by controlling the class environment (measuring physical environment parameters), and by embedding knowledge within objects and automatically adjusting local conditions to improve the effectiveness of study [9, 46, 71, 72]. |

IoT technologies, such as those listed in the table above, have the potential to shift the marketplace from a technology innovation experiment to a compelling business strategy by: (a) unlocking the excess capacity of physical assets; (b) creating a liquid and transparent marketplace; (c) enabling radical re-pricing of credit and risk; (d) improving operational efficiency; and (e) digitally integrating value chains [59]. For the business-related IoT prospects, recognising the importance of opportunities and adjusting their strategies according to the market and users' preferences will improve the performance of organisations. In addition, business operations will be transformed as, by digitalising and connecting physical assets to the IoT, it will become feasible to search, utilise and engage with them [59].

### *5.2 Service Innovation: Benefits and Opportunities*

The IoT shows great potential for changing the existing industrial and business processes, and unlocking economic and market values [54, 73, 74]. In the future economy, driven by knowledge, innovations enabled by revitalised products and processes are potentially one of the driving factors which strengthen financial and competitive advantages [75]. In organisations, the value created by the IoT systems and applications determines their adoption, for instance in providing customized services to their customers [75]. In addition, the IoT opens a number of opportunities to connect activities, resources, and actors in business networks [25]. This connected world reveals great market potential when it comes to improving efficiency, and

transforming production [29].

Integrating the IoT in organisations accelerates value creation and improves customer services, in particular, by applying the customer service life cycle (CSLC) framework, which is enhanced by digital data streams formed by the mass adoption of IoT devices [76]. This stream of real-time data is enabled by identifying, sensing, communicating and computing the capabilities of IoT devices, and is another way to add value for businesses since information processing is necessary in each stage of the service life cycle [76]. The use of the CSLC framework in information systems helps companies to better understand and improve customer services by exploiting the IoT innovations at different stages, i.e. understanding customers' requirements and preferences, improving the distribution approach, enhancing customers' experience in using and maintaining and fulfilling the needs for transfer or disposal after use [76].

Fleisch [28] identified seven economic value drivers, which can be grouped by their root causes based on machine to machine communication and the integration of users; this may offer a way to make sense of value enablers. The first group includes the simplified manual and automatic proximity trigger, automatic sensor triggering, and automatic product security. By enabling smart things with identification, interaction, monitoring and cryptography, these applications contribute to increasing the transaction and processing speed, accuracy, convenience, product and service quality, as well as the level of security. Business organisations can simplify the effort of employees, and enable customer self-service, increasing their perceived convenience and trust, and it can reduce security and labour costs, resulting in operation optimisation. The second group of value drivers refers to direct, extensive, and mind changing user feedback. Smart things can provide direct feedback to the users, serve as links to various services, and influence the behaviour of customers. Hence, business operations can get accurate and direct feedback from users, resulting in additional business opportunities and add-on services [28]. However, these seven value drivers are thoroughly reviewed in 2016 by Nolin and Olson from the perspective of "alpha convenience" (the convenience that is enabled by the IoT, which depicts a vision of ubiquitous connectivity), possible problems addressed by each of them are identified, for example, the lack of privacy, the unnecessary personalisation that restricts the decision making of users, and the decreased autonomy of owners of smart devices [77].

The innovation diffusion process is analysed by the Henderson and Clark model in manufacturing, which clearly explained the evolutionary impact of the IoT. They suggest that the diffusion process of IoT follows the radical, modular, architectural, and incremental stages [78]. For example, the uniquely identified items (e.g. RFID) will drive IoT in the first stage and related products could be developed; consequentially, data flow could be formulated, which shapes an environment for products in the next stages [78]. Given that the evolutionary path influenced by the IoT for manufacturing has been clarified, businesses could capture the value and navigate the technological shift in order to obtain competitive advantage [78]. In organisations, IoT diffusion comprises five levels [28]. The first, basic, level is defined as using IoT technology as a diagnostic tool that identifies problems with newly available information. The next level refers to the companies that simply automate, rather than improve, their business

processes. The third level is defined as organisations that have modified business routines enabled by IoT. Firms in the next level integrated their offerings with IoT value drivers to create new possibilities. Lastly, the highest level represents companies transforming their business models based on absolute visibility enabled by IoT technologies. For example, a company can switch its business paradigms from simply selling products to renting its products to customers on a pay-per-use basis [28]. This innovation measurement method is comparatively fundamental, but requires training in the approach by which company innovation is classified. A *"depth of diffusion"* measurement instrument was developed in the context of logistics based on a combination of an intelligent product classification model and the analysis of qualitative research results [38]. This measurement includes six identification characteristics (**Error! Reference source not found.**) [38]. All of the characteristics are used to examine the adopted IoT technologies of a particular company. The levels of each indicator should be identified by assessing the functions of their logistic technologies [38].

**Table 2 Measurement of the Depth of Diffusion [38]**

| **Level** | **1** | **2** | **3** |
|---|---|---|---|
| Usage of technology | Auto ID | Sensors | Embedded system |
| Energy Supply | Induction | Accumulator | Self-sustained |
| Connectivity | Manual readout | On demand | Continuously |
| Information processing capacity | Storage | Message | Decision-making |
| Aggregation level | Packing level | Object level | Component |
| Location of intelligence | Network | Object | Distributed |

Beyond this, enlarging data collection in future networks and offering smart services enabled by networked sensors are two main characteristics of the IoT that enable service innovations [48]. The increasing number of connected nodes exponentially increases the power and economic value of networks, with IoT infrastructure acting as a dynamic end-to-end information network, turning data into useful information [48]. The connection between the physical and virtual world provides valuable information that plays a major role in service innovation. To this end, five important capabilities of IoT applications have been identified that need to be considered when designing new products and services: (a) sensing and sharing the location information and then providing services based on the location; (b) collecting and processing physical or chemical environmental information; (c) controlling IoT terminals and executing functions remotely based on the information and requirements; (d) self-organised networking and interoperating with the network layer; (e) communicating securely [36].

A conceptual framework of network dynamics in IoT-enabled service innovation processes has also been proposed to explain the interactions between the identified determinants [25]. In this framework, the four innovation processes determining variables are summarised as

*"overlapping"*, *"intermediating"*, *"objection of actors"*, and *"business modelling"*. Overlapping refers to the changing process of connectivity and interdependence between networks that influence the network structure, actors' positions, and conditions for network coordination [25]. From a business network perspective, all actors, activities, and resources can be regarded as intermediaries in the networking process that engage in transformation. The evolution of IoT technologies leads to an increasing role of intelligent devices in peoples' lives and organisational activities. In analysing IoT innovations, the objects can be included as actors in network processes [25]. Among the determinants of service innovation, the business model attracts most of the attention. Given that the business model is a mediating factor between technology and economic value and that it acts as a plan of service provision and revenue realisation, the business model should be in harmony with the other actors in the process [25]. Enterprises need to define or redefine their business models to specific applications and sectors in order to align them to different fast growth technology-leading trends, to create superior value, and to achieve a competitive advantage in the intensive global competition [45, 73, 79, 80]. The IoT can have an impact on business models by innovating the old ones and facilitating the development of creative new ones that are sustainable in the long term [81]. The core building blocks of business model development in IoT-driven ecosystems are value proposition (the source of opportunities that contribute to the revenue streams), value co-creation (all monetary and non-monetary benefits that attract collaborators in the ecosystem), and value network (relationship with key partners, customers, and all remaining stakeholders) [45, 82, 83]. Also, the IoT could enhance knowledge sharing, by connecting not only people, but also objects, with intelligence [84]. IoT can open a series of opportunities when it comes to improving knowledge management and innovation capacity, which can help create new value for organizations [74]. The knowledge management enhanced by IoT can contribute to more than enlarging innovation capacity, but also in terms of facilitating the decision making process, marketing, consumer engagement, and branding for businesses [84].

Beyond the service innovation, the IoT creates value by improving brand warmth, brand competence, as well as the brand attachment perceived by the customers [85]. The interaction style between a company and their target customers determines the audiences' understanding and evaluation of the services. The findings show that a friend-like interaction style enabled by the smart and responsive attributes of the IoT significantly improves consumers' perception of a brand's intentions and their ability to induce intentions, namely the brand warmth and competence, hence increasing the emotional attachment between the consumers and the brand. Specifically, a friend-like interaction, which refers to the interaction style that creates agreeable experiences and close relationships by indicating caring intentions and exposing positive traits such as sincerity, honesty and genuineness, is superior to an engineer-like style (a precise and attentive communication style which conveys an expert-like image to consumers) in enhancing brand value, especially for companies with a friendly brand positioning [85].

In addition to service and operation improvements facilitated by IoT, potential opportunities for investment also facilitate the growth of innovative enterprises [37]. The intellectual capital which determines a company's economic value is enabled by the human capital (knowledge workers), structural capital (patents that improve the products and services) and relational capital (network of stakeholders) [86]. It is suggested that for companies,

investments in IoT will lead to increases in intellectual capital and economic value [86]. The value of IoT technologies for investments arises from flexibility. The typical net present value approach, which ignores flexibility in investment, such as reversibility and scalability, is no longer appropriate [33]. The real option valuation approach, which takes actions during a period of time, is particularly valuable in high uncertainty and risk industries in IoT contexts. There are four types of real options: (a) to abandon/switch from an operating loss project; (b) to scale back an operating loss project; (c) to defer/postpone something, to wait and see if a project will be profitable; (d) to expand/scale up a successful project [33]. Decision trees are used as a valuation method to calculate the real option value since this allows *"setting up possibilities of the project according to what management believes them to be"* [33]. The valuation is based on five variables, namely, present value, investment cost, uncertainty of a project, the time window of the project, and the time value of money [33].

### *5.3 Strategy and Operations*

The future product design concept needs to be customer-centric, as customer experience will be an essential offering of the IoT [59]. Internet connected objects (ICO) will equip companies with unlimited consumption and contextual information by indicating their customers' unobservable characteristics and product usage patterns based on observed behaviour [19]. This provides opportunities to customise strategies and offer personalised products to customers by an efficient supply chain. Based on this, *"tailoring"* and *"platform"* strategies are proposed as future supply chain management practices [19]. These two types of customisation strategies are recommended to product suppliers in the era of IoT: (a) the tailoring strategy refers to the ability of the provider to produce multiple tailored products to meet customers' demand; (b) the platform strategy refers to the ability of the supplier to produce a standardised but flexible product/platform that can incorporate personal ICO data and allows customers to purchase additional custom-made products made by other providers which are compatible with the platform, thus ICO products could be customised continuously while being used [19]. These strategies can become profitable through maximising consumers' value. With increasing demand for contextual variety, the platform strategy becomes more profitable, relative to the tailoring strategy [19].

As far as the logistics operation for service providers in improving their competitiveness is concerned, the IoT can be used in providing *"autonomous, self-controlled transport of logistic objects from the sender to the consignee"* [38]. The supply chain is one of the areas that benefits from the IoT on a large scale. The management and innovation could be transformed into a connected world with integrated data, resources, activities, and processes [87]. The value creation mechanism of IoT technology can generate information which facilitates the optimisation of business process flows, industrial processes, predictive maintenance, providing efficient service solutions [75]. The information sharing capability of the IoT increases efficiency in the supply chains of various industries. For example, the IoT helps operators of agricultural products in inspecting and delivery via an EPC information system based on RFID [88]. Yu et al. [89] developed a conceptual model to study the relation between delivery service provider selection and customer satisfaction in the e-retailing industry context. Their work associates organisational competitiveness with logistics service providers, which enhances

information and material flows along the supply chain [89]. Their model refers to the assets-process-performance framework, which facilitates the understanding of organisational competitiveness in a combination of assets, processes and performance and is established by defining the soft and hard infrastructure of delivery service providers as assets, the flexibility of supply chains as the process, and customer satisfaction as organisational performance [89]. Flexibility is defined as *"the process of adapting things based on the customer requirement"* and is assessed as a general capability of a firm, while the definition of customer satisfaction is a series of psychological states resulting when the emotion surrounding disconfirmed expectations is combined with their prior experience [89]. Results show that soft and hard infrastructure mediated by flexibilities improves customer satisfaction, but neither soft nor hard infrastructure can directly improve customer satisfaction. Therefore, the competitiveness at the firm level is enhanced by satisfying their customers in the product delivery process, which is determined by the service providers' infrastructure and flexibility.

Usage of warehouses is essential for all suppliers, manufacturers, and retailers due to the requirements for responsive and flexible supply chains led by economic globalisation and growing supply chain interdependence [90]. The industrial deployment of IoT infrastructure provides an ideal order fulfilment platform, called collaborative warehouse platforms [90]. This logistic platform facilitates the sharing of physical space and logistic information by several producers and distribution companies, which improves the global performance of overall distribution processes [90]. Warehouse visibility, traceability, and transparency can be improved to facilitate the competitiveness in a dynamic environment by utilising this ideal platform for decentralised warehouse management [90].

IoT technologies do not only contribute to the operation and management of business enterprises, but they also benefit social organisations such as hospitals. For instance, the healthcare industry can optimise inventory and asset management procedures by utilising IoT technologies in tracking and tracing objects, data mining, information collection and utilisation [3]. Following the roadmap of healthcare by IoT technologies from 2010 to 2020 developed by Man et al. [3], studies in this domain have considered leveraging IoT technologies in medical asset management, optimising medical resources, monitoring the healthcare situation, and home healthcare. The availability of increasing cheap wearable, implanted, and environmental sensors and RFID evokes the potential to develop personal Smart-Health systems and to produce and manage participatory medical knowledge [70].

### *5.4 Security, Accountability and Ethical Design*

Underlying privacy and security challenges and issues need to be addressed in order to optimise the delivery of the benefits and value of IoT products to users. In the operation of IoT, security is critical at both the physical devices level and the service/applications level; each of the layers in IoT architecture (i.e. the sensing, network, service, and interface layers) addresses potential threats and appropriate actions should be taken (i.e. general device, communication, network, and application security) [91]. Even though legislation is required in order to secure the information in terms of privacy, confidentiality, integrity, authenticity, and availability of use [50], protection can be achieved by system security and ethical design processes in business

units.

In organisations, one of the main concerns is organised crime and cyber terrorism since manufacturing facilities, critical infrastructure (e.g. the power grid, oil pipelines, nuclear power plants, and railway systems), personal smart homes, as well as intellectual property, are all linked in the IoT world [35]. In other words, given its nature, the IoT generates a large amount of data, information and knowledge that is collected and transferred between the virtual and physical world, hence it could be the source of potential safety issues [4, 22]. Threats to security arise from each of the layers in IoT architecture: for example, unauthorised access and authentication difficulties of physical devices act as the end-node of IoT; spoofing and routing attacks, and viruses, Trojans, and junk messages in data transmission; privacy leakage and service abuse in the service and application layer [91]. The difficulty in analysing security problems derives from the broad dimensions of the IoT with various usage cases and risk scenarios [35].

*"Security includes …[protection from]… illegal access to information and attacks causing physical disruptions in service availability"* [50]. Potential security issues are driven by the incapability in the implementation of complex schemes, due to the low capacity of the connected devices, the physical accessibility to the components and objects due to the lack of attention and open access to the systems [7, 9]. IoT devices are defined as devices with processing and communication capabilities, including equipment and appliances in different application domains [16, 72]. Previous literature suggests that 70% of the commonly used IoT devices are vulnerable because of the lack of transport encryption, inadequate software protection, web interface insecurity, and insufficient authorisation [33]. Currently available solutions are proposed regarding computing systems and sensor networks, though with implementation problems and unsatisfactory security [9]. On the other hand, improvement in the accountability in the IoT supports security and confirms the need for a stable legal framework for businesses [92]. Accountability can be defined as the obligation of a person (who is accountable) to explain and justify their actions or decisions to another person (the accountee) [92]. This has to be developed in a multi-stakeholder approach, since the IoT should cope with various segments of society [63]. As business transactions and information exchange are carried out through global information architecture in an IoT context, it is essential to clarify who is responsible once a system fault occurs [92]. IoT applications have further demands in terms of privacy, accessibility, and transparency that human actors have limited capability to satisfy [39]. A theoretical framework that explains the way in which IoT technologies can enable or constrain actors' control capabilities in satisfying the accountability demands has been proposed by Boos et al. (2013) [39]. This associates accountabilities, control capabilities, and the capacity of IoT as three multi-dimensional constructs which interact with each other. Each of these involves three dimensions: the accountability is measured by visibility, responsibility and liability; the concept of control is defined as *"an actor's ability to influence conditions and processes conducive to goal fulfilment"*, which contains the dimensions of transparency, predictability and influence; and the capacity of IoT is assessed by examining the effects on automating, informing and transforming work processes [39]. This framework is helpful in examining the influences of the design decisions regarding potential organisational challenges [39].

Popescul and Georgescu [22] pointed out that the ethical dangers of the IoT must be appropriately managed to prevent danger for individuals and organisations. These dangers originate from enabling technologies and the characteristics of applications. Eight characteristics and five widely applied technologies (i.e. Sensors, RFID, NFC, GPS, and 3G/4G) have been identified, leading to four potential ethical issues [22]. The most common ethical issues in relation to IoT are identified from four aspects with key concerns: privacy (enforce the right to a private life by restricting the revelation of information), accuracy (ensure the information's authenticity, integrity and responsibility), ownership (enforce the right of information owning), and accessibility (ensure the right to obtain specific information) [22, 61]. These ethical issues are in line with the four key privacy concerns introduced earlier [61]. One of the vital ethical challenges regarding the ownership right of personal data and information appears with the identification. The development of objects equipped with sensors enables them to collect and send data in large quantities and in different ways through the internet without human intervention [22]. From an economic point of view, ethical challenges come from the *"conscious choices resulting from misplaced incentives"*, due to which the economic incentives of business organisations depend on creating applications or devices collecting the users' data instead of protecting it, especially in the trading of users' data between businesses [4].

These issues arise from the characteristics of the IoT as sensing and networking technologies facilitate IoT scenarios. Popescul and Georgescu [22] summarised eight IoT characteristics that may drive ethical issues, from a report of the European Commission [93]: (a) ubiquity and pervasiveness: once the users are engulfed and immersed in IoT, there is no clear way to opt out or give up; (b) miniaturisation and invisibility: the computers, as well as other devices, will become invisible to human sight due to several characteristics of the sensors such as their small size, and transparency; (c) ambiguity: criteria of identity and system boundaries will be ambiguous because of the difficulties in distinguishing natural objects, artefacts, and human beings as a result of easy transformation from one type to another by the means of tagging, engineering and absorption into a networks of artefacts; (d) identification: all objects will have unique identities in the IoT world, thus the authority of assigning, administering and managing these identities will be a crucial governance issue in the globalising world; (e) ultra-connectivity: the high degree of production and transfer of data between humans and objects in the connected world might cause serious problems if they are used maliciously; (f) autonomous and unpredictable behaviour: a hybrid system will be constituted by human and interconnected objects in which humans will be part of IoT environments with the devices and artefacts, thus unexpected behaviours without the users' full understanding will emerge; (g) incorporation of intelligence: the smart and dynamic objects will be extensions of the human mind and body, people might feel socially and cognitively handicapped without access to the intelligent and data carrying IoT environment; (h) distributed control: the control of IoT will not be centralised due to the vast number of data, nodes, and hubs. The monitoring and governance of emerging phenomena and properties have implications for accountability and the control of activities [22, 93]. Essential features of ethically designed products have been discussed, aimed at reducing the risks of investing in products and services, supporting long-term relationships with customers who wish to buy ethically-framed products and use better services, and helping to create a society in which people have a high-level trust

in using the IoT [4]. An IoT product based on ethical design should have four features: (a) capability to provide control over agency, awareness, and reflexivity in the data collection and distribution to the users; (b) capability to implement different regulations over time and space; (c) capability to support dynamic contexts; (d) capability to perceive and support ethical choices [4]. The process of the development of IoT products is summarised in four steps. Firstly, it is necessary to understand and include the need for trust in the application, product, and service users at both public and private levels. Then, the involvement of the users in the design process helps to translate and include their needs and values into the product or service. Thirdly, the simplicity and transparency of data collection, usage, storage, and accessibility should be demonstrated and comprehended by the users. Lastly, a legal framework and accountability of the users' privacy and trust should be established to better enhance the IoT environment [4].

## 6 Conclusions and Future Research Avenues

The paper has offered a systematic review of business related IoT studies. We first presented the main definitions of IoT and identified a number of distinctive characteristics. Then, by identifying journal articles from three databases and by following a rigorous review process, we discussed and critically synthesised the findings under two themes, namely, the user and organisational perspectives. The next three sections discuss the theoretical and practical implications as well as the main limitations of our work.

### *6.1 Theoretical contribution*

The main theoretical contribution of this paper is in the form of future research avenues which have been generated by the analysis of the previous literature. On the individual level, future research could explore how IoT will shape consumers' consumption habits and to what extent users will engage with such products and services. Current research emphasises the users' acceptance, adoption, and use behaviour towards IoT services and applications, which will provide implications for companies in formulating their business strategies to attract better adoption (e.g. [56]), thus accelerating IoT implementation. More empirical studies on general IoT services and specific tasks are required. Due to the technology-centric nature of IoT offerings, most current studies on users' perceptions are based on technology acceptance theories. In addition, buying, using and continuance intentions are also closely associated with product development and life cycle management in terms of object functions and value proposition. Overall, potential emphases for future research are the development of research frameworks of use behaviour specific to the IoT context, and new IoT product characteristics and development processes.

From the organisations' perspective, potential research topics could examine: the essential capabilities of the products and applications that better enhance users' experiences; the way in which the IoT can engage with the supply chain strategy of personalised products; the degree to which the application of IoT technologies will optimise company operations; and the general R&D process and requirements. The changing market influenced by the engagement of emerging technologies and dynamic consumers' preferences have a crucial role in the development of products and services. Intellectual resources such as knowledge, information

and ideas are key elements in the IoT era because of the increasing importance of creative industries [37]. Creativity enabled by novel technologies will be a vital driver in company growth and significantly foster economic success. It leads consumers' preferences to shift to personalised products that can be provided by effective supply chains or that are capable of being customised by platforms. As the users are gaining importance in product development, the acceptance and adoption of IoT applications and the experimental study of customised services are worth further investigation. In the implementation of IoT a consistent vision from individuals and organisations will facilitate fast growth, since the fast deployment of objects enabled with sensors can significantly increase the pervasiveness and connectivity that shape the environment for users and enable innovation processes for businesses.

Recent studies have focused on and discussed the approaches to controlling and reducing the potential risks in order to inspire the full potential of the IoT. Individuals, organisations, and governments should share consistent stances on issues concerning the invasion of human privacy, attacks on security systems, and ethical violations. For instance, with regard to privacy, the control of private information is required by users, which will encourage governments to introduce appropriate legislation that organisations should follow in product and service design. Future research could focus on the importance of providing feasible prevention and solutions to risks and could identify the principles that could be followed in developing strategies, including laws, regulations, policies, as well as technological solutions toward the systems and their architecture.

Referring to the pervasive nature of the IoT, the automatically generated data which initiate and realise IoT services will be based on an integrated global infrastructure. Current studies focus on proposing an information framework, experimental deployments, and analysing potential influences. We have identified two research questions that originated from the data flow and IoT construction: specifically, how to automatically sense, collect, use, manage, and protect the data; and the realisation and construction of IoT infrastructure on large scales, for instance, the smart city. Finally, by combining visions of the IoT with the above-mentioned topics, worldwide powerful influences and impacts will be brought about by the IoT in the near future. Potential research avenues are shifts in government policies, the global economy, societal and cultural characteristics, and individuals' psychological changes.

### *6.2. Managerial Implications*

This study provides a range of managerial implications. Firstly, when it comes to acceptance and adoption, users are very concerned with privacy protection and the security of their assets. Organisations need to invest more effort in both ensuring research and development and the need to bring products to market quickly, while not compromising on safeguarding user privacy. They should also invest more effort not only proactively informing customers of potential implications but also educate them more broadly when it comes to managing their IoT services and platforms. Ease of use should not be considered in the context of individual products and services but as a whole, so that users can maximise the benefits they gain from IoT, by exploiting the synergies among different products and services. Developing robust IoT standards will make it possible to minimise uncertainty and encourage new companies to enter

the market. In turn this will accelerate the innovation process and result in new products and service as well as extending the options that customers have to choose among. Internally, managers can look at IoT as an opportunity for attaining new levels of efficiency and effectiveness. Facilitating the diffusion of IoT technologies/systems in organisations enhances the innovation process and optimises the operations, creatively involving them in IoT innovations and equipping IoT technologies so that they properly benefit the company in the long run.

### *6.3. Limitations*

Our work also has some limitations. Specifically, the review of the previous literature could have followed a more quantitative approach, based on a meta-analysis of the main concepts identified by the review of the papers in order to examine the interrelationships and potential causal effects between them. In addition, the authors could have involved more experts in the selection and the evaluation of the papers by following a Delphi approach in order to increase reliability and validity. Finally, our literature search was limited to business related subject categories in academic journals and therefore some papers which have been published in other subject categories of academic journals may have been ignored even though they have business related implications.

## References

[1] P. Guillemin and P. Friess, Internet of things strategic research roadmap. The Cluster of European Research Projects, in, Technical report, 2009.

[2] UK Research Council, Research in the wild - Internet of Things 2013, in, 2013.

[3] L. C. K. Man, C. M. Na and N. C. Kit, IoT-based Asset Management System for Healthcare-related Industries, International Journal of Engineering Business Management, 7 (2015).

[4] G. Baldini, M. Botterman, R. Neisse and M. Tallacchini, Ethical Design in the Internet of Things, Science and Engineering Ethics, (2016) 1-21.

[5] D. Kreps and K. Kimppa, Theorising Web 3.0: ICTs in a changing society, Information Technology and People, 28 (2015) 726-741.

[6] D. Shin, A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things, Telematics and Informatics, 31 (2014) 519-531.

[7] J. A. Stankovic, Research Directions for the Internet of Things, IEEE Internet of Things Journal, 1 (2014) 3 - 9.

[8] N. Olson, J. M. Nolin and G. Nelhans, Semantic web, ubiquitous computing, or internet of things? A macro-analysis of scholarly publications, Journal of Documentation, 71 (2015) 884-916.

[9] L. Atzori, A. Iera and G. Morabito, The Internet of Things: A survey, Comput. Networks, 54 (2010) 2787-2805.

[10] S. Li, L. D. Xu and S. Zhao, The internet of things: a survey, Information Systems Frontiers, 17 (2014) 243-259.

[11] B. N. Yan, T. S. Lee and T. P. Lee, Mapping the intellectual structure of the Internet of Things (IoT) field (2000–2014): a co-word analysis, Scientometrics, 105 (2015) 1285-1300.

[12] D. Mishra, A. Gunasekaran, S. J. Childe, T. Papadopoulos, R. Dubey and S. Wamba, Vision, applications and future challenges of Internet of Things: A bibliometric study of the recent literature, Industrial Management and Data Systems, 116 (2016) 1331-1355.

[13] A. Mehmood, G. S. Choi, O. F. von Feigenblatt and H. W. Park, Proving ground for social network analysis in the emerging research area "Internet of Things" (IoT), Scientometrics, 109 (2016) 185-201.

[14] D. Tranfield, D. Denyer and P. Smart, Towards a methodology for developing evidence-informed management knowledge by means of systematic review, British journal of management, 14 (2003) 207-222.

[15] F. Hasson, S. Keeney and H. McKenna, Research guidelines for the Delphi survey technique, Journal of advanced nursing, 32 (2000) 1008-1015.

[16] ITU-T, Y.2060: Next Generation Networks - Frameworks and Functional Architecture Models, in: Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks, Telecommunication Standardization Sector of ITU, 2012.

[17] ITU Strategy and Policy Unit. , ITU Internet Reports 2005: The internet of things, Geneva: International Telecommunication Union (ITU), (2005).

[18] L. Yang, S. H. Yang and L. Plotnick, How the internet of things technology enhances emergency response operations, Technological Forecasting and Social Change, 80 (2013) 1854-1867.

[19] I. Ng, K. Scharf, G. Pogrebna and R. Maull, Contextual variety, Internet-of-Things and the choice of tailoring over platform: Mass customisation strategy in supply chain management, International Journal of Production Economics, 159 (2015) 76-87.

[20] P.-L. P. Rau, E. Huang, M. Mao, Q. Gao, C. Feng and Y. Zhang, Exploring interactive style and user experience design for social web of things of Chinese users: A case study in Beijing, International Journal of Human-Computer Studies, 80 (2015) 24-35.

[21] S. Evdokimov, B. Fabian, O. Günther, L. Ivantysynova and H. Ziekow, RFID and the Internet of Things: Technology, applications, and security challenges, Foundations and Trends in Technology, Information and Operations Management, 4 (2011) 105-185.

[22] D. Popescul and M. Georgescu, Internet of Things - Some Ethical Issues, USV Annals of Economics & Public Administration, 13 (2013) 208-214.

[23] A. J. Jara, M. C. Parra and A. F. Skarmeta, Participative marketing: Extending social media marketing through the identification and interaction capabilities from the Internet of things, Personal and Ubiquitous Computing, 18 (2014) 997-1011.

[24] V. Ng, The future of enterprise mobility -- enterprise IoT?, NetworkWorld Asia, 11 (2014) 10-12.

[25] P. Andersson and L.-G. Mattsson, Service innovations enabled by the "internet of things", IMP Journal, 9 (2015) 85-106.

[26] F. Salim and U. Haque, Urban computing in the wild: A survey on large scale participation and citizen engagement with ubiquitous computing, cyber physical systems, and Internet of Things, International Journal of Human Computer Studies, 81 (2015) 31-48.

[27] W. Zhou and S. Piramuthu, Information Relevance Model of Customized Privacy for IoT, Journal of Business Ethics, 131 (2015) 19-30.

[28] E. Fleisch, What is the Internet of Things? An Economic Perspective, Economics, Management & Financial Markets, 5 (2010) 125-157.

[29] R. James, Out of the box - Freescale: How free models scale in the world of information, Business Information Review, 29 (2012) 95-98.

[30] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, Internet of Things for Smart Cities, IEEE Internet of Things Journal, 1 (2014) 22-32.

[31] Y. Chang, X. Dong and W. Sun, Influence of characteristics of the internet of things on consumer purchase intention, Social Behavior and Personality, 42 (2014) 321-330.

[32] J. Jin, J. Gubbi, S. Marusic and M. Palaniswami, An Information Framework for Creating a Smart City Through Internet of Things IEEE Internet of Things Journal, 1 (2014).

[33] I. Lee and K. Lee, The Internet of Things (IoT): Applications, investments, and challenges for enterprises, Business Horizons, 58 (2015) 431-440.

[34] H. Wang, T. Zhang, Y. Quan and R. Dong, Research on the framework of the Environmental Internet of Things, International Journal of Sustainable Development and World Ecology, 20 (2013) 199-204.

[35] T. Bradley, P. Thibodeau and V. Ng, The Internet of Things -- threats and challenges, NetworkWorld Asia, 11 (2014) 16-18.

[36] S. Chen, H. Xu, D. Liu, B. Hu and H. Wang, A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective IEEE Internet of Things Journal, 1 (2014) 349 - 359.

[37] A. Sofronijević, V. Milićević and B. Ilić, Smart City as Framework for Creating Competitive Advantages in International Business Management, Management (1820-0222), (2014) 5-15.

[38] A. Bremer, Diffusion of the "internet of things" on the world of skilled work and resulting consequences for the man-machine interaction, Empirical Research in Vocational Education and Training, 7 (2015).

[39] D. Boos, H. Guenter, G. Grote and K. Kinder, Controllable accountabilities: The Internet of Things and its challenges for organisations, Behaviour and Information Technology, 32

(2013) 449-467.

[40] J. S. Winter, Surveillance in ubiquitous network societies: Normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things, Ethics and Information Technology, 16 (2014) 27-41.

[41] M. Tuters and K. Varnelis, Beyond locative media: Giving shape to the internet of things, Leonardo, 39 (2006) 357-363.

[42] J. Zhao, X. Zheng, R. Dong and G. Shao, The planning, construction, and management toward sustainable cities in China needs the Environmental Internet of Things, International Journal of Sustainable Development and World Ecology, 20 (2013) 195-198.

[43] A. Bassi and G. Horn, Internet of Things in 2020 - Roadmap for the Future, in: G. Santucci, P. Friess and T. Sommer (Eds.) European Commission: Information Society and Media, European Commision, 2008.

[44] D. E. O'Leary, 'Big Data', the 'Internet of Things' and the 'Internet of Signs', Intelligent Systems in Accounting, Finance and Management, 20 (2013) 53-65.

[45] U. Gretzel, M. Sigala, Z. Xiang and C. Koo, Smart tourism: foundations and developments, Electronic Markets, 25 (2015) 179-188.

[46] N. Dlodlo, T. Foko, P. Mvelase and S. Mathaba, The State of Affairs in Internet of Things Research, Electronic Journal of Information Systems Evaluation, 15 (2012) 244-258.

[47] C. Speed, An internet of old things, Digital Creativity, 21 (2010) 239-246.

[48] X. Xu, Internet of things in service innovation, Amfiteatru Economic, 14 (2012) 698-719.

[49] M. Quigley and M. Burke, Low-cost internet of things digital technology adoption in SMEs, International Journal of Management Practice, 6 (2013) 153-164.

[50] A. S. Elmaghraby and M. M. Losavio, Cyber security challenges in smart cities: Safety, security and privacy, Journal of Advanced Research, 5 (2014) 491-497.

[51] J. Brill, The internet of things: Building trust and maximizing benefits through consumer control, Fordham Law Review, 83 (2014) 205-217.

[52] B. D. Weinberg, G. R. Milne, Y. G. Andonova and F. M. Hajjat, Internet of Things: Convenience vs. privacy and secrecy, Business Horizons, (2015).

[53] L. Gao and X. Bai, A unified perspective on the factors influencing consumer acceptance of internet of things technology, Asia Pacific Journal of Marketing and Logistics, 26 (2014) 211-231.

[54] S. Kim and S. Kim, A multi-criteria approach toward discovering killer IoT application in Korea, Technological Forecasting and Social Change, 102 (2016) 143-155.

[55] A. Y.-L. Chong, M. J. Liu, J. Luo and O. Keng-Boon, Predicting RFID adoption in healthcare supply chain from the perspectives of users, International Journal of Production Economics, 159 (2015) 66-75.

[56] H. Bao, A. Yee-Loong Chong, K.-B. Ooi and B. Lin, Are Chinese consumers ready to adopt mobile smart home? An empirical analysis, International Journal of Mobile Communications, 12 (2014) 496-511.

[57] C. L. Hsu and J. C. C. Lin, An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives, Computers in Human Behavior, 62 (2016) 516-527.

[58] M. S. Balaji and S. K. Roy, Value co-creation with Internet of things technology in the retail industry, Journal of Marketing Management, (2016) 1-25.

[59] P. Brody and V. Pureswaran, The next digital gold rush: How the internet of things will create liquid, transparent markets, Strategy and Leadership, 43 (2015) 36-41.

[60] V. Ng, Drivers and obstacles to IoT adoption in Asia Pacific, NetworkWorld Asia, 11 (2014) 12-14.

[61] X. Caron, R. Bosua, S. B. Maynard and A. Ahmad, The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective, Computer Law & Security Review, 32 (2016) 4-15.

[62] A. M. Ortiz, D. Hussein, S. Park, S. N. Han and N. Crespi, The Cluster Between Internet of Things and Social Networks: Review and Research Challenges IEEE Internet of Things Journal, 1 (2014) 206 - 215.

[63] R. H. Weber, Internet of things - Governance quo vadis?, Computer Law and Security Review, 29 (2013) 341-347.

[64] R. H. Weber, Internet of things - Need for a new legal environment?, Computer Law and Security Review, 25 (2009) 522-527.

[65] R. H. Weber, Internet of things: Privacy issues revisited, Computer Law and Security Review, 31 (2015) 618-627.

[66] G. Del Chiappa and R. Baggio, Knowledge transfer in smart tourism destinations: Analyzing the effects of a network structure, Journal of Destination Marketing & Management, (2015).

[67] S. R. Babu and S. Subramoniam, Tourism Management in Internet of Things Era, Journal of Information Technology & Economic Development, 7 (2016) 1-14.

[68] B. L. Risteska Stojkoska and K. V. Trivodaliev, A review of Internet of Things for smart home: Challenges and solutions, Journal of Cleaner Production, 140 (2017) 1454-1464.

[69] L. L. Kiesling, The connected home and an electricity-Market platform for the twenty-First century, Independent Review, 20 (2016) 405-409.

[70] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi and G. Marrocco, RFID Technology for IoT-Based Personal Healthcare in Smart Spaces IEEE Internet of Things Journal, 1 (2014) 144- 152.

[71] G. Adorni, M. Coccoli and I. Torre, Semantic web and internet of things supporting enhanced learning, Journal of E-Learning and Knowledge Society, 8 (2012) 23-32.

[72] A. Uzelac, N. Gligoric and S. Krco, A comprehensive study of parameters in physical environment that impact students' focus during lecture using Internet of Things, Computers in Human Behavior, 53 (2015) 427-434.

[73] W. H. Dutton, Putting things to work: Social and policy challenges for the Internet of things, Info, 16 (2014) 1-21.

[74] G. Santoro, D. Vrontis, A. Thrassou and L. Dezi, The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity, Technological Forecasting and Social Change, (2017).

[75] M. Del Giudice, Discovering the Internet of Things (IoT) within the business process management: A literature review on technological revitalization, Business Process Management Journal, 22 (2016) 263-270.

[76] B. Ives, B. Palese and J. A. Rodriguez, Enhancing Customer Service through the Internet of Things and Digital Data Streams, MIS Quarterly Executive, 15 (2016) 279-297.

[77] J. Nolin and N. Olson, The Internet of Things and convenience, Internet Research, 26 (2016) 360-376.

[78] A. Caputo, G. Marzi and M. M. Pellegrini, The Internet of Things in manufacturing innovation processes: Development and application of a conceptual framework, Business Process Management Journal, 22 (2016) 383-402.

[79] P. Pisano, M. Pironti and A. Rieple, Identify Innovative Business Models: Can Innovative Business Models Enable Players to React to Ongoing or Unpredictable Trends?, Entrepreneurship Research Journal, 5 (2015) 181-199.

[80] M. Chui, M. Löffler and R. Roberts, The internet of things, McKinsey Q., (2010) 70-79.

[81] T. J. Gerpott and S. May, Integration of Internet of Things components into a firm's offering portfolio – a business development framework, Info, 18 (2016) 53-63.

[82] R. M. Dijkman, B. Sprenkels, T. Peeters and A. Janssen, Business models for the Internet of Things, International Journal of Information Management, 35 (2015) 672-678.

[83] S. Turber, J. vom Brocke, O. Gassmann and E. Fleisch, Designing Business Models in the Era of Internet of Things: Towards a Reference Framework, in: M. C. Tremblay (Ed.) International Conference on Design Science Research in Information Systems, Springer, 2014, pp. 17-31.

[84] L. Solima, M. R. Della Peruta and M. Del Giudice, Object-Generated Content and Knowledge Sharing: the Forthcoming Impact of the Internet of Things, Journal of the Knowledge Economy, 7 (2016) 738-752.

[85] J. Wu, J. Chen and W. Dou, The Internet of Things and interaction style: the effect of smart interaction on brand attachment, Journal of Marketing Management, (2016) 1-15.

[86] A. Murray, A. Papa, B. Cuozzo and G. Russo, Evaluating the innovation of the Internet of Things: Empirical evidence from the intellectual capital assessment, Business Process Management Journal, 22 (2016) 341-356.

[87] B. Li and Y. Li, INTERNET OF THINGS DRIVES SUPPLY CHAIN INNOVATION: A RESEARCH FRAMEWORK, International Journal of Organizational Innovation, 9 (2017) 71-92.

[88] B. Yan, C. Yan, C. Ke and X. Tan, Information sharing in supply chain of agricultural products based on the Internet of Things, Industrial Management and Data Systems, 116 (2016) 1397-1416.

[89] J. Yu, N. Subramanian, K. Ning and D. Edwards, Product delivery service provider selection and customer satisfaction in the era of internet of things: A Chinese e-retailers' perspective, International Journal of Production Economics, 159 (2015) 104-116.

[90] P. J. Reaidy, A. Gunasekaran and A. Spalanzani, Bottom-up approach based on Internet of Things for order fulfillment in a collaborative warehousing environment, International Journal of Production Economics, 159 (2015) 29-40.

[91] S. Li, T. Tryfonas and H. Li, The Internet of Things: a security point of view, Internet Research, 26 (2016) 337-359.

[92] R. H. Weber, Accountability in the Internet of Things, Computer Law and Security Review, 27 (2011) 133-138.

[93] J. Van den Hoven, Fact sheet- Ethics Subgroup IoT - Version 4.0, in: Conclusions of the Internet of Things public consultation, European Commission, 2013.