Chapter 3
Smart Cities on the Cloud

Christina Kakderi, Panagiotis Tsarchopoulos, Nicos Komninos and Anastasia Panori

Abstract The emergence of the cloud computing paradigm has found fertile ground in the smart cities discipline, especially with regards to its benefits both in terms of big data storage and analytic capabilities and in terms of smart city service provision. Over the past years we have noticed an abundance of publications on cloud computing; from government reports to corporate studies, all show the significant benefits of cloud computing and the opportunities presented by the migration of public/municipal services to the cloud. Despite the availability of information, the landscape with regard to cloud computing adoption is still quite blurry. This chapter aims to provide methodological guidance to public/city authorities on the use of and the actual steps towards taking up the cloud computing paradigm. More specifically, it offers a simple methodology in the form of a roadmap with the main roadblocks one can expect to encounter when migrating public services to the cloud, along with a set of recommendations that facilitate decision-making in various stages of this process. We also argue that cloud computing adoption should not be an isolated action of an organization (city authority/governmental agency), but part of a wider strategic model based on open innovation practices (the use of open source technologies for the cloud platform and applications, the use of open data, the adoption of user engagement methodologies etc.) as well as the use of innovative business models.

C. Kakderi (✉) · P. Tsarchopoulos · A. Panori
Urban and Regional Innovation Research (URENIO), Aristotle University of Thessaloniki, Thessaloniki, Greece
e-mail: christina@urenio.org

P. Tsarchopoulos
e-mail: patsar@auth.gr

A. Panori
e-mail: apanori@urenio.org

N. Komninos
School of Engineering, Aristotle University of Thessaloniki, Thessaloniki, Greece
e-mail: komninos@urenio.org

A. Stratigea and D. Kavroudakis (eds.), *Mediterranean Cities and Island Communities*, Progress in IS, https://doi.org/10.1007/978-3-319-99444-4_3

Keywords Smart cities · Cloud computing · Migration to the cloud
Cloud platform · Applications

3.1 Introduction

Cloud computing has received significant attention over the last decade especially with regards to the benefits it creates in the case of large organizations with high levels of complexity and limited financial and operational resources. Despite the emergence of a large volume of scientific publications as well as of corporate and governmental reports on the subject, the landscape with regards to cloud computing adoption is still quite blurry. First, there is not a clear picture on how city authorities can practically document the benefits to be enjoyed from cloud computing. This does not only refer to monitoring the changes in the performance and cost of stand-alone applications, but also to documenting the overall impact on their organizational efficiency and smart city strategic goals. Second, there is limited evidence on how city authorities can overcome the main challenges that appear due to the transition of their services to the cloud. One might think that leveraging cloud computing would only require the existence of technical capabilities on the part of the public authority. Nevertheless, there are many more challenges that have to be addressed; institutional and legislative limitations or organizational deficiencies are only a few of many. Also, as cloud computing adoption is not a one-step process, but rather a selection among multiple route paths and levels of engagement or acceptance, the development of a cloud migration strategy is far from 'a one size fits all' plan. Therefore, city authorities must fully comprehend the rich but mostly fragmented information they have in order to develop their own strategy that will reflect a series of choices on multidimensional aspects.

Cloud Computing entails significant operational and financial benefits to cities, allowing them—among other things—to select, adapt and re-use ready-made and tested smart city services/solutions. Besides, cities worldwide face more or less the same socio-economic and environmental challenges. Nowadays hundreds of applications exist (open source or proprietary) that try to cope with complex urban problems such as traffic management, environmental pollution, safety and security and so on in cities (Komninos et al. 2014). The challenge therefore is not to develop smart city services, but to prioritise needs, leverage new technologies and capitalise on different business models.

This implies that cloud computing alone is not sufficient to transition to this state of 'smartness'. Besides, the potential of smart cities lies not only in the use of ICT infrastructure and the development of digital services but also in the redefinition of their innovation ecosystem with the aim of establishing and nurturing structures for collaborative intelligence (Komninos et al. 2012). During recent years, cities in Europe and the rest of the world have been urged to attract external resources and involve various actors in dealing with urban problems. We are witnessing cities embracing a culture of 'openness' through the adoption of open innovation, the use of open data or the development and sharing of open source smart city applications. Tsarchopoulos et al. (2017) discuss the adoption of open innovation practices in smart cities through: (i) the establishment of collaborative communities with the aim of crowdsourcing ideas and/or effort in addressing complex urban problems, (ii) the formation of competitive communities such as hackathons and smart city application development contests, and (iii) the development and offering of applications which target common urban problems through open online repositories with the aim of them being to be reused by other cities. Lastly, the adoption of new technologies leads to the emergence of innovative business models that depart from traditional models of infrastructure financing; and reveal new business opportunities and complex relationships among the stakeholders and the financial system (Hamilton and Zhu 2017; Díaz-Díaz et al. 2017).

Building on this discourse we concur with the organizational and financial benefits that cloud computing provides to city authorities in order to achieve their smart city vision. Our aim in this chapter is to provide methodological guidance on the use and the actual steps required in taking up the cloud computing paradigm. More specifically, we offer a simple methodology in the form of a roadmap with the main roadblocks encountered when migrating public services to the cloud, along with a set of recommendations that facilitate decision-making in various stages of this process. We also argue that cloud computing alone is not sufficient and that the added value of its benefits can only be maximised once it is combined with a broader strategy for smart city development. In other words, cloud computing adoption should not be an isolated action of an organisation (city authority/governmental agency), but part of a wider strategic model based on open innovation practices (the use of open source technologies for the cloud platform and applications, the use of open data, the adoption of user engagement methodologies, etc.) as well as the use of innovative business models.

This chapter is organised into four sections. After the introductory section where we describe the context and general problem on which this work is focused, the second section reviews the literature on cloud computing and the way it is connected to the smart cities literature. The section ends with a description of the STORM Clouds[1] platform and services (a H2020 project outcome) and the overall methodological experiment on migrating smart city applications to the cloud. The third section describes in a detailed set of sequential steps and sub-steps the process of migrating public services to the cloud and provides a set of recommendations targeted to city authorities that ensure the success of this task. The final section highlights that in order to fully reap the benefits of the 'smartness' paradigm, public authorities have to adopt a wider set of strategic choices apart from just leveraging cloud computing. These choices refer, among others, to the use of open data, the creation and sharing of new data or the adoption of user engagement methodologies.

[1]STORM CLOUDS Project, http://stormclouds.eu/. Accessed 20 December 2017.

3.2 Smart Cities and Cloud Computing: A New Pair of Concepts in the Recent Literature

3.2.1 Cloud Computing Definition and Implementation

Cloud Computing (CC) has received considerable attention over the last decade as an emerging paradigm beyond a simple computing system structure (Kakderi et al. 2016a; Seo et al. 2014). In simplified terms, it can be understood as the possibility to store, process and use data on remotely located computers accessed over the Internet (EC 2012). *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (Mell and Grance 2011: 2). Therefore, it is an all-inclusive solution based on the concepts of converged infrastructure, shared services/resources and dynamic reallocation based on demand, which has the potential to bring significant benefits to its users (citizens, businesses, government), such as cost savings, increased efficiency, user-friendliness, accelerated innovation (Mahmood 2016; ECPSB 2014).

Cloud computing can be classified on the basis of targeted service and its prospective use (Zhang et al. 2010; Seo et al. 2014) in four main types: public clouds, private clouds, hybrid clouds and community clouds. Nowadays, one can find numerous reports and contributions providing a detailed description of the prevailing categories, which may altogether be referred to as the Cloud Computing Stack: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). A simplified description of what each one of these categories entails is that: (a) SaaS applications are designed for the end-users and are delivered over the web, (b) PaaS is the set of tools and services designed to make it easy to code and deploy these applications in a quick and efficient way, and (c) IaaS is the hardware and software (servers, storage, networks, operating systems) that powers all the above (Tsarchopoulos et al. 2017).

As a technology and an industry, cloud computing seems to have reached a certain level of maturity, allowing for full commercial exploitation. It is estimated that, with the right policy framework, the cloud economy could generate nearly 1 trillion in GDP and 4 million jobs by 2020 in Europe (IDC 2012). A KPMG study for Australia shows that the increased adoption of cloud computing in the country would lead to a growth of annual GDP by $3.3 by 2020 (KPMG 2012). At the global level, IDC estimates that it can create $1.1 trillion of business revenues per year. Although it is now established in the technology toolbox, the rationale for using cloud continues to evolve (Miller et al. 2018). In fact, as shown by Fig. 3.1, it is not the technology itself that has sparked a growing interest in the academic literature, but its unlimited implementation in the field of smart cities.

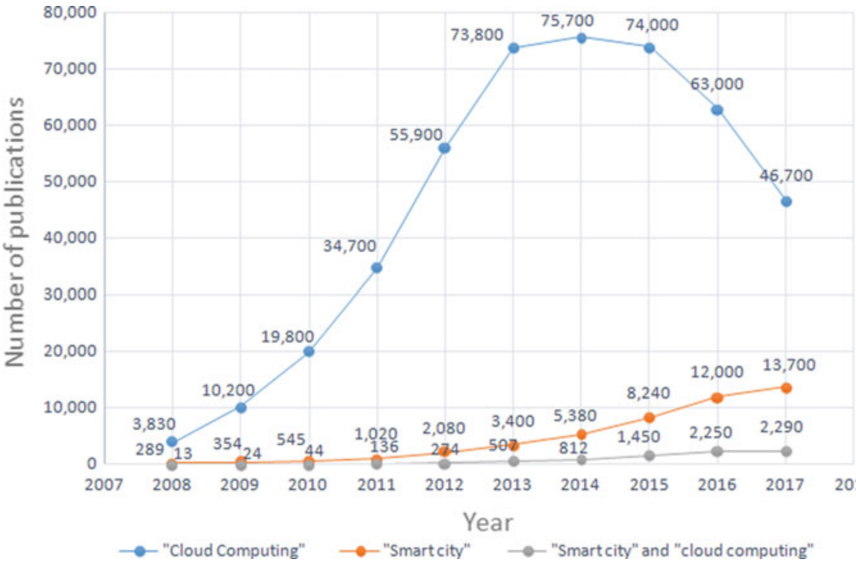

Fig. 3.1 The evolution of academic publications on CC and CC in smart cities. *Source* Own elaboration based on Google search data (2008–2017)

3.2.2 The Field of Smart Cities

Smart cities is a particularly popular concept that has emerged since the beginning of the millennium, covering a wide range of scientific disciplines including urban planning, computer science and sociology to name just a few (Mora et al. 2017). It reflects both the vision of a new generation of cities and a new planning paradigm (Komninos 2015) towards more efficient and sustainable cities that offer a high quality of life to their citizens. The concept does not limit itself to the use of new technologies that create efficiencies for urban problems. Technology is just an enabler empowering emergent innovation ecosystems in the urban space to create collective intelligence (Schaffers et al. 2011).

The popularity of the concept has led cities worldwide to adopt smart city strategies and develop services for their citizens, focusing on different city domains (economy, infrastructures, governance etc.) that deal with various challenges of the urban environment (investment attraction and entrepreneurship, mobility, waste management, etc.) (Komninos 2015). This task can be overwhelming in terms of IT infrastructures and capabilities. Due to high technological requirements, many multinational technology and consultant companies have found fertile ground to become involved not only by developing technology products and solutions, but also by shaping the theoretical framework and research agenda in the field of smart cities (Komninos 2015). The market potential is almost unlimited. According to a report by Global Industry analysts in 2016, the global market for smart cities is projected to reach $1.2 trillion by 2020.[2]

3.2.3 Cloud Computing and Smart Cities

Cloud computing seems to have a key role to play in the development of smart cities. Among the numerous corporate reports and scientific papers, we can distinguish some efforts to combine the two notions. A special issue on smart cities and cloud computing that was recently published (Kakderi et al. 2016b) discussed the main pillars for developing or migrating smart city services to the cloud: the design and development of the Cloud environment, the selection and adaptation of the services that are most suitable for the selected Cloud environment, and the use of data mining and analytics in order to gain insights from the data on the cloud. Besides this, a couple of reports and EU-funded research projects, such as EPIC and STORM Clouds reflect the interest in the decisions that city authorities have to face as they transition to the cloud, and have tried to address obstacles that hinder the use or contribute to the slow uptake of cloud technologies, especially within their smart city strategy.

The attention on the coupling of these two notions can be attributed to two strands of literature. The first strand has to do with the nature of city authorities as complex organisations and the benefits that cloud computing creates for entities with such an extended size and scope of services. More specifically, most city authorities are very complex in nature with many entities (departments, agencies etc.) sharing large volumes of data, but also have rigid organisational structures and significant funding restrictions in terms of innovation. They also encompass services in diverse business and technological domains, which are often based on monolithic architecture models, disconnected from each other and difficult to re-use (EC 2014). In recent years many city authorities have been seeking out new ways to improve their service quality and delivery, transparency, responsiveness as well as the effectiveness of their investments, hence there is an increasing interest in cloud computing. The concept of cloud computing is not only relevant due to its significant benefits, such as coherence, flexibility and economies of scale; it is also linked to the idea of open, connected and re-usable public services (EC 2014). According to Hamilton and Zhu (2017) the more fundamental services available on the cloud, i.e. basic public services, the higher the opportunity to re-use and combine them with existing services from other governmental departments or to develop new services in collaboration with third parties (Angelidou et al. 2017; Komninos et al. 2016).

[2] http://www.strategyr.com/MarketResearch/Smart_Cities_Market_Trends.asp. Accessed 4 April 2018.

The second strand of the literature has to do with the challenges that city authorities face in their effort to deal with urban problems. To do that, they have to collect and manage an enormous amount of heterogeneous data coming from a variety of sources (sensors and other devices, smartphones, domestic appliances, etc.). They also have to be able to analyse these data and extract meaningful insights that can be used in their smart city operations. Kakderi et al. (2016b) describe the need for cloud computing in smart cities in three main areas: (i) the facilitation of big data storage, processing, mining and analytics as well as visualisation integrating various objects in IoT, (ii) the ability for virtualisation which abstracts the physical infrastructures and creates various dedicated resources according to user needs, and (iii) the applicability of all three service models (IaaS, SaaS and PaaS) of cloud computing to smart city solutions.

The main impacts of cloud computing in service delivery are that it reduces the need for internal resources (cost, time), enables the provision of more integrated and user centric services, improves agility and transparency and facilitates the development of innovative services (Deloitte 2011; Chandrasekaran and Kapoor 2011). Mahmood (2016 xvii) has summarised the benefits of cloud computing adoption by public organisations by grouping them in two categories: the ones that address the public organization themselves and the ones that address citizens. More specifically, governments can have improved management; cost and time savings; more precise and timely information; automation; easy maintenance and upgrading of services; and harmonious collaboration with other governmental departments whether vertical or horizontal. Citizens, on the other hand, have access to easy-to-use and on demand e-services; reliable and timely information and services available around the clock; opportunities for participation in decision-making, also through digital means.

Despite the significant benefits described above, there are a number of reasons cloud adoption is not occurring more rapidly in the public sector. Many challenges relate to its newness and the relative underdevelopment of the marketplace for cloud services (Craig et al. 2009). The most common concerns are related to security and data protection, privacy, portability and interoperability. However, there are also some organizational challenges that public authorities have to consider before moving their services to the cloud. The first is related to the *lack of flexibility in public procurement*. Public authorities can use their procurement weight in order to promote the development and uptake of cloud computing based on open technologies and secure platforms (EC 2012). However, IT budgets in the public sector are usually planned in advance, allowing little flexibility for last minute changes. The second refers to the *lack of uniformity in standards* across nations. Contrasting rules on privacy, security, storage and accessibility create difficulties for cloud providers in delivering on the full promise of information technology (West 2010). Finally, there are some *cultural problems* which emerge from the fact that different organizations—or departments within the same organization—are not used to collaborating or sharing solutions with each other.

3.2.4 Cloudification of Smart City Services

Cloud migration is an application landscape redesign that changes not only the way IT administrators interact with the public organization's systems but also the way applications interact with each other and are delivered to end-users (Brophy 2016). The decision to migrate an application to the cloud requires a very deep understanding of the application architecture, the operational requirements, the business requirements, and the security requirements in order to make the most well-informed decisions (EPA 2017).

The fundamental issue public authorities face, when moving to the cloud, is the identification and implementation of the appropriate strategy, which meets the aims of their organization whilst enjoying the cloud's significant benefits. Migrating to the cloud raises many questions and poses a number of risks for organizations if not handled correctly. As it has already been mentioned, published reports review the main aspects of cloud computing, however, the exact way in which such a task can be undertaken is still an unknown process. In fact, there is not a single strategy: a public service organization can choose to be one of three things; a user, a provider or both. The complexity also derives from the fact that all key players, such as regional governments, citizens and service providers, can get involved (Accenture 2013).

The migration of public services and applications to the cloud should be done in a strategic and methodological manner, after considering a large number of key aspects, such as the cost of migration, application redesign, application performance and availability, security and privacy requirements, regulatory requirements, etc. (CSCC 2018). Although there is not a single path, planning for cloud migration should entail careful preparation and a defined strategy in a form of a roadmap that will act as a guide, as well as a checklist with technical, managerial, financial and other considerations.

The following section presents some useful guidelines on how to address the process of moving towards a cloud-based solution for public authorities and policy makers. We use the experience gained from STORM Clouds,[3] an EU co-funded CIP project, which aimed to accelerate the pace at which public authorities move to cloud computing.[4] The guidelines that are presented below have been prepared

[3]STORM CLOUDS Project, viewed December 20, 2017, http://stormclouds.eu/.

[4]Some of the core elements of the project, which facilitated this experimentation, are the following:

(i) A cloud-based platform that provides the environment to host the smart city applications. The STORM Clouds Platform (SCP) is a layered cloud architecture that is based on open source technologies (Battara et al. 2016). The platform provides an advanced and customizable IaaS solution that supports both public and private cloud deployment models, facilitating the deployment of civic applications in a cloud environment.

(ii) A list of cloud-related services, such as security and data protection, resource monitoring, automation etc.

based on direct experimentation in 4 European cities (i.e. Thessaloniki, Valladolid, Agueda, Miscolc), creating a set of relevant use cases and best practices that allow public authorities to take full advantage of the cloud computing model.

3.3 A Roadmap for the Migration of Public Services to the Cloud

Drawing on the experience gained from this project we have created a roadmap that aims to help public authorities in their migration to the cloud. The roadmap provides a set of guidelines with regards to the technical, organizational and business challenges in the transition of smart city services to the cloud. An illustration of the roadmap can be found in Fig. 3.2.

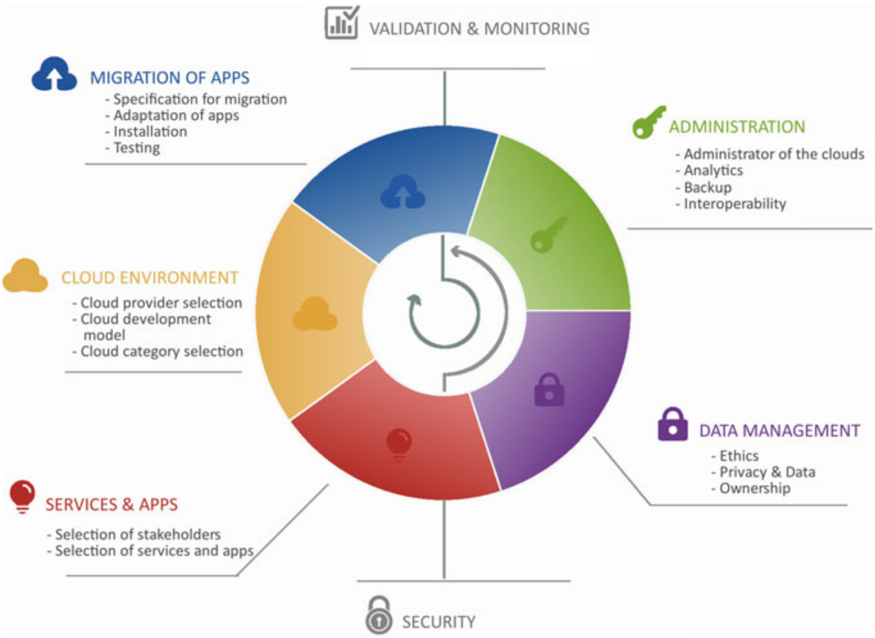

Fig. 3.2 A roadmap for planning public services' migration to cloud computing. *Source* Own elaboration

(iii) A portfolio of consolidated and interoperable open-source cloud-based smart city services that cover a variety of city functions, such as the innovation economy, city governance and quality of life. These services can be easily transferred and adapted to other cities. This process can be facilitated with the use of the SCP and the accompanied services as well as with the methodological guide provided below in the form of a roadmap.

The roadmap includes five sequential steps (services and applications, cloud environment, migration of applications, cloud administration, data management) and two parallel procedures (security and validation/monitoring). We argue that these steps represent the main roadblocks that public authorities have to face and for each one we provide guidance, either by describing a case study solution or by providing a set of recommendations/guidelines.

3.3.1 Step 1—Services and Applications

The *first step* in the roadmap starts with the *identification and engagement of the stakeholders* that will participate in this user-driven process as well as the *selection of the most suitable services* to be cloudified.

Step 1a. Selection and engagement of stakeholders

Engagement strategies should start from the first stages of the migration process in a series of iteration cycles that should include the following steps:

i. The identification and classification of stakeholders according to the type of services, in order to involve as many as possible. Stakeholders might be internal to the public organisation itself, such as groups of employees or departments (legal, IT, budget/financial, procurement), but also external, such as community groups, business associations, NGOs, Cloud Service Providers, etc.
ii. Segmentation of stakeholders based on their level of interest and influence as well as definition of the roles and potential responsibilities. As not all of them can contribute to the same degree, public authorities should also identify which ones are expected to influence the service by acting as co-creators, as contributors or as users.
iii. Mapping or creating and utilising (digital and traditional) tools and methods that will enable continuous collaboration with stakeholders. Different stakeholders might need to be contacted via different communication channels (e.g. newsletters, social networks, personal meetings and working groups). Also, different tools might be used for different levels of engagement (information, consultation, training, etc.).
iv. Analysing different elements in order to prevent potential problems and defining contingency strategies (Table 3.1). For example, cloud migration might trigger a reluctance to change among some employees; therefore change of management processes might be needed.

Step 1b. Selection of the services to be cloudified

Before transitioning to the Cloud, it is vital that public authorities first determine which applications better fit into the Cloud environment. Identifying and prioritizing the best applications to be moved to the cloud means considering and analyzing different factors that have to do with the service/app itself (architecture,

Table 3.1 Method to identify cloud migration risks and define contingency plans *Source* Own elaboration

Element	Risk	Contingency plan
Technical staff	Feel that their job is at risk and don't collaborate in the migration process	Training sessions to improve their skills so they can work with the cloud Job redefinition
Management	The resources required for the project are not provided	Apply long-term reasoning to show that a current investment will bring future savings

design, potential usage, technical and legal specifications, etc.), the experience and expectations of the responsible organization, dependence on third party software, etc. The selection of services should primarily be made based on the organization's objectives and needs, and for this, internal reviews might provide important insight. However, in general terms, the most suitable ones are applications that make the most of the elasticity of Cloud Computing and can lead to significant financial savings.

For each of the services identified, one must collect information on the technologies currently in use such as the operating system, programming language, databases, web/app services, frameworks, application lifecycle tools and whether the app exists (or not) in an open source repository. Migrating services to the cloud implies the possibility of other city authorities accessing services and transferring them without the need to develop them from the scratch. Such a task includes analysis of a different set of criteria such as: (i) documentation, (ii) target users, (iii) flexibility, (iv) language, (v) compliance with internal security regulations, and (vi) specifications.

3.3.2 Step 2—Cloud Environment

The decision on the Cloud environment which comes as a *second step*, relates to *cloud service category selection* (IaaS, PaaS, SaaS), the *selection of the cloud development model* (public, private, hybrid, community) and technologies as well as the *selection of the Cloud Service Provider*. The available choices in this step have mostly been analysed in the recent literature.

Step 2a. Cloud service category selection

With regards to cloud service category selection, each of the available services (IaaS, PaaS, SaaS) has its own specific implication for using it. SaaS describes the most abstract layer of the cloud stack and it is more suitable if the organization wants ready-made online applications, although it cannot be applied if one is migrating an existing application to the cloud. Usually, most common choices involve a combination of SaaS and IaaS as public authorities first concentrate on the infrastructure (Bonneau et al. 2013). If public authorities want to migrate their own applications to the cloud, they have to select between IaaS and PaaS, both of which enable the extension of platforms so that public authorities' IT can respond proactively and reactively to increased demand for services at a lower cost (VMware 2011). IaaS is the most flexible (as it does not require any architectural changes to be made to the applications or to have full control of the resources for deployment) albeit a more complex solution, given that it requires prior installation and configuration of all the components for high availability and scalability. PaaS on the other hand offers the cloud infrastructure and manages levels of scalability, software upgrades and maintenance, although it might require significant changes to the applications (Tsarchopoulos et al. 2017).

Step 2b. Cloud deployment model selection

To select the best cloud deployment model (public, private or hybrid), the organization has to make a number of decisions with regards to the level of control, security requirements, and cost. While public clouds may be the best option for smaller organizations with limited funds, private or hybrid clouds, which offer more control and/or security, are more suitable for larger organizations with available manpower and a budget to manage those deployments effectively.

Step 2c. Cloud service provider selection

As public authorities shift to cloud computing, they have to choose a cloud provider to host their cloud-based virtual machines. The choice of a Cloud Service Provider (CSP) requires evaluation of an extensive list of options, such as:

- *Service Levels* as public authorities in most cases have strict needs regarding availability, response time, capacity and support. Cloud Service Level Agreements (CSLA) establish a clear contractual relationship between a cloud service customer and a Cloud Service Provider of a cloud service.
- *Support* could be offered online or through a call centre, and in some cases, it could be necessary to refer to a dedicated resource with precise timing constraints.
- *Security*. When a public entity enters the cloud, it is entrusting its information assets to a third party provider. Although normally the potential supplier should follow recognised security policies in line with industry best practice, city authorities have to be able to assess essential features regarding the security level offered by providers such as the mechanisms in place to preserve client applications and data.
- *Privacy* i.e. the legal requirements for the protection of the personal data hosted in the cloud service, including issues such where the CSP's data will be located, including any trans-border data transfers, if applicable.
- *Open Standards* in order to avoid getting locked into cloud infrastructure that has restrictive contracts or proprietary technologies.
- *Compatibility* meaning that the cloudified applications have to fit into the CSP's existing pre-configured templates. The CSP's architecture should also meet scalability, availability, capacity and performance guarantees and should be sufficient for agency requirements.

- *Interoperability* enabling workloads to span multiple environments. For greater interoperability value, it is best to look for a provider that offers a common infrastructure platform for public and private hosted clouds, as well as an on-premises private cloud (Frost and Sullivan 2011).
- *Pricing* given that the complexity of the pricing formulas makes it very difficult to estimate the cost for each service in order to be able to make a meaningful comparison (Posey 2015). The terms of the contract, payment methods and payment dates can be decisive factors as well. City authorities should validate the cost model against the CSP's pricing by considering the following (Australian Government 2011): (i) the transparency of the pricing system, e.g. subscription or pay-as-you-go pricing, upgrades, maintenance and exit costs, (ii) potential costs for unexpected peaks in demand, (iii) service prices for upgrade and maintenance fees appropriate to the services being procured; some upgrades may be automatic and included in the service, (iv) suitability of the cost model allowing for scaling and changes to service, (v) commitment requirements, such as minimum use, (vi) setup, training and integration fees and (vii) the ongoing cost of service.
- *Redundancy* as adequate backup procedures and robust disaster recovery plans must be incorporated into the cloud offering.
- *Easy-to-use administration environment*, which refers to a user-friendly client portal that allows administrative tasks to be carried out or storage space or services to be added quickly.

3.3.3 Step 3—Migration of Applications

Third comes migration of application, i.e. the process of redeploying an application, typically to newer platforms and infrastructure.

Step 3a. Specifications for migration

This is a multifaceted process, which begins with an assessment of the hosting environment already in use. The analysis covers both the network (e.g. configuration, connectivity requirements from the city authority's premises to the Cloud environment, and supplementary services such as SMTP, DNS and WWW) and architecture (e.g. use of resources, underlining technologies, licences, and security mechanisms) of the service. Together with the hosting environment it is crucial to analyse the applications' readiness for the cloud. Aspects such as customisation, regulatory compliance, complex service architectures and service maturity need to be carefully investigated, as they could negatively impact the cloudification process. A critical aspect is the availability of both the application's source code and documentation (installation manual, code dependencies, required software packages, etc.).

Next, public authorities should define the functional and technical characteristics of the Virtual Machines that will host the applications in the new Cloud

Environment. The analysis of the functional requirements covers technical details (e.g. Operating System, Scripting Language, Database, Web/Application Server, Data Formats, Frameworks/Libraries and External Services used), interoperability issues, and static characteristics, such as hard-coded IP addresses and directory paths. Furthermore, the analysis of the non-functional requirements addresses issues related to the proper functioning of the application, such as security, regulatory compliance, performance, availability, backup, privacy, reusability, and interoperability. An estimation of the use of resources regarding RAM, Disk Space, CPUs, Bandwidth, Hits/Month, Registered Users, Max Online Users, and Average Online Users helps calculate the expected workload per application. An important characteristic that should be examined in this step is whether the application's design supports its deployment on multiple servers. In that case the application will take full advantage of the performance benefits that the cloud offers.

This analysis of the functional and technical requirements also highlights potential obstacles to the transformation or the porting of the applications to the cloud due to technical or functional reasons. For example, applications implemented with legacy technologies might require licenses in order to use commercial software products. When porting an application to the cloud, one should make sure that it does not constitute an infringement of the licensing rights that the application proprietors have in place with the software vendor. From a functional point of view, a potential problem might be the use of sensitive information, such as personal data that could raise privacy and security issues. In addition to the implementation of extensive security controls like unauthorised access prevention, data encryption and an ad hoc firewall policy, there still remain questions about where the data are located.

Step 3b. Adaptation of the applications

The applications that have been selected for migration to the Cloud may require significant changes to take full advantage of Cloud characteristics. Applications should be re-designed in order to take full advantage of the Cloud's features, especially when: (i) hardware cost is substantial, (ii) IT staffing levels are low, as moving to the cloud automates a lot of server and application management, as well as maintenance tasks that would otherwise be performed by in-house IT staff, (iii) geolocation is a requirement, (iv) the application needs to scale for predicted, but infrequent, uptime as the cloud allows systems that have occasional spikes to quickly and easily scale servers on demand without an expensive hardware investment or footprint. Determining the right migration strategy for an application depends on its level of cloud alignment, cloud readiness, the potential benefits achieved from migrating, and the risks entailed.

Step 3c. Installation

The next step in the migration process is deployment in the new environment. Depending on the type of workload being considered and the type of target Cloud environment chosen, migration might be moving from the non-Cloud environment to the Cloud environment, cross-platform migration or application-only migration (Writer 2013). During the migration process considerations arise with regards to privacy, interoperability, data integrity, data application portability and security, which may cause a high level of complexity. Over recent years a large number of online tools and services have helped to simplify this process. Automated tools can help design the Cloud environment and plan the migration. Such tools may be of general purpose or application specific. Most common are automated tools that help with setting up the replication of Virtual Machines from on-premises installations to the cloud, such as OpenStack Heat.

Step 3d. Testing

Cloud scalability does not always eliminate application performance problems, and even after migrating to the cloud applications might not scale up correctly (Pelerin 2015). Performance testing aims to ensure that the deployed applications are fully functional and that they meet the initial set of requirements regarding cloudification. It also helps to solve issues such as database errors or application and website crashes. Testing should be done periodically and include general performance and compatibility tests, stress and load tests and security/vulnerability tests.

3.3.4 Step 4—Administration of the Cloud

The fourth step is the administration of the cloud.

Step 4a. Administration of the cloud

Due to the characteristics of the cloud, system administrators no longer need to provide servers, install software and wire up network devices, since all this work is replaced by a few clicks and command line calls. Nowadays, most of the daily tasks performed by system administrators are related to the applications. The Cloud environment should offer both system administrators and application owners the necessary tools required to manage and maintain the platform and the deployed applications. Using these tools, they can focus on how to optimise the cloud-based application in order to increase cost savings.

Step 4b. Analytics

Administration platforms are usually accompanied by monitoring tools that facilitate data analysis in order to find meaningful insights and empower administrators with knowledge that lets them optimise their cloud systems. Monitoring tools are used for cloud monitoring, performance management, automation, cost management, etc. Over recent years, a number of cloud monitoring tools have been developed including Nagios, Prometheus and Zabbix (open source), CloudMonix, New Relic, AppDynamics, etc. These provide the ability to collect and visualise information using table and graphs, analyse historical trends, create alerts and perform a variety of functions from a single web-based console.

Step 4c. Backup

Administration of the cloud also includes backup, which is the process of making a secondary copy of data that can be restored to use if the primary copy (the production copy, which is the official working copy of the data) becomes lost or unusable. Backups usually comprise a point-in-time copy of primary data taken on a repeated cycle—be it daily, monthly or weekly. It is the most important means of keeping the data from being lost due to intentional or unintentional access. It is also important to encrypt the up-to-date backups. Backup is the easiest and the most familiar process for most situations. A backup copy is used to recover data needed to restart an application correctly. Backups may be required in the following scenarios:

- *Logical corruption.* This can happen due to application software bugs, storage software bugs or hardware failure, such as a server crash.
- *User error.* Where an end user may accidentally or intentionally delete a file or directory, a set of emails or even records from an application.
- *Hardware failure.* In the form of hard disk drive (HDD) or flash drive failure, server failure or storage array failure.
- *Hardware loss.* Possibly the worst case scenario where an event such as a fire results in hardware being inoperable and permanently unrecoverable.

Step 4d. Interoperability

Finally, issues of interoperability should be solved, which can be understood as how well a public administration service interacts with external entities in order to organize the efficient provisioning of its public services to other public administrations, businesses and or citizens. Some recommendations for interoperability include the following:

- Each interoperability attribute differentiates between at least two maturity levels.
- The improvement tables provide recommendations on how to improve maturity step-by-step for a specific interoperability attribute.
- When a public service does not have the maximum level yet for a specific interoperability attribute, a recommendation is given to make the move towards the next interoperability level.
- When a public service does have the maximum level for an interoperability attribute, no recommendation is given.
- When the foreseen maturity improvement is a sliding scale (e.g. from less to more), a generic recommendation (not maturity level specific) is given to improve the maturity further along the sliding scale.

3.3.5 Step 5—Data Management

The next phase is related to the administration of the cloud, including issues of *ethics*, *privacy* and *data* as well as *ownership*.

Step 5a. Ethics

In terms of ethical issues, it is recommended that an ethical issues' strategy should be based on the following three tasks:

- Proactivity: It is vital that all parties involved in cloud computing are proactive, in order to anticipate unforeseeable consequences. Players should never use uncertainty to refrain from designing and providing services that invite morally sound use and inhibit undesirable or controversial actions. It is thus recommended as ethical for Cloud providers to have a *Terms and Conditions* available and for users to know the Terms and Conditions offered by providers.
- *Regulations and policies*: All technology should be subjected to regulation arrangements at least just enough to have innovation that can benefit society and not enough to limit innovation. In any case, regulations can have ethics integrated into technological development and use. It is vital that governance arrangements are more conducive to the inclusion of ethics; this should also cover regulations for private companies, which are usually much less subject to ethics-related oversight and are more geared towards profit generation. Such regulations will adapt as cloud computing evolves. In any case, it is important to remember the core definition of corporate responsibility and follow policies defined by the European Union, such as the ISO26000 standard.
- *Responsible Research and Innovation*: Responsible Research and Innovation (RRI) is of a particular importance. It can be defined as an inclusive approach to Research & Innovation (R&I), aiming at better aligning both the process and outcomes of R&I with the values, needs, and expectations of society, notably through reinforcing public engagement, open access, gender dimension, ethical issues, and (formal and informal science) education.

Step 5b. Privacy and data protection

Privacy is understood as the right of a person to have his/her personal data properly secured. Moreover, it is related with the ability of persons to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others (ICO 2014). Data protection is the process of safeguarding important information from corruption and/or loss (Microsoft 2014).

Cloud services make it easier for public authorities to take advantage of opportunities to share information. For example, sharing personal information with another public authority or agency may be achieved by simply creating user accounts with the appropriate permissions within a SaaS solution rather than having to implement a system-to-system interface to exchange information. Although cloud services have the potential to lower the technical barriers to information sharing, public authorities must ensure that they appropriately manage access to personal information and comply with the requirements of the European and national privacy legislation.

Step 5c. Ownership

Cloud providers should commit to protecting the data and limit the use thereof. The data that public authorities host in cloud services belongs to them and should not be used by a cloud provider for purposes other than to provide the customer's service. Moreover, cloud providers should not use customer data for purposes unrelated to providing the service, such as advertising. Additionally, each service has established a set of standards for storing and backing up data, and securely deleting data upon request from the customer.

The best-designed and implemented service cannot protect customer data and privacy if it is deployed in an environment that is not secure. Customers expect that their data will not be exposed to other cloud customers. They also assume that the processes used at the data centre, and the people who work there, all contribute to keeping their data private and secure.

Despite the five sequential phases, we have two more horizontal issues described here: (i) cloud security which refers to policies, technologies, and controls deployed to protect data, applications and the associated infrastructure, and (ii) monitoring and validation, which targets the business aspect of application migration.

3.3.6 Security

Cloud computing security refers to the broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure (EC 2015). As cloud computing technology and business models evolve, each year a number of publications appear with new recommendations on this issue (ENISA 2009; CSA 2016; UKCloud 2016). There are a number of security concerns associated with cloud computing, which can be broadly grouped into: (a) issues faced by Cloud Service Providers who have to ensure that their infrastructure is secure and clients' data and applications are protected; and (b) issues faced by their customers, who have to make sure that their provider has taken appropriate security measures to protect their information. The security expectations and obligations for both sides are described in Service Level Agreements (SLAs) (Gianakoulias 2016).

It is essential that public authorities understand the specific security requirements of each application they want to migrate to the cloud, especially with regards to data protection, audits, etc. To achieve this, they should map every application that is a candidate for migration to cloud computing to a set of security, governance, and compliance issues that are specific to that application. This will enable them to understand the application requirements, and how the migration and re-development effort to the cloud could impact application operations (Tsarchopoulos et al. 2016).

The UK's National Technical Authority for Information Assurance, which provides advice on Information Assurance Architecture and cyber-security to the UK government and the wider public sector and suppliers to the UK government, published 14 security principles to consider when evaluating cloud services, such as protection for data in transit; operational, personnel and supply chain security; governance framework, identity and authentication; service management and service administration, etc. (Cloud Security Guidance 2016). Consumers of Cloud services should decide which of the principles are important, and how much assurance they require in implementing these principles, while providers of cloud services should consider these principles when presenting their offerings to public sector consumers. This will allow consumers to make informed choices about which services are appropriate for their needs.

3.3.7 Validation and Monitoring

As Tsarchopoulos et al. (2017) mention, monitoring and validation target the business aspects of applications rather than the technological ones. Validation can be done from different perspectives, such as:

- Validation of the services deployed. This includes the service itself, utilising feedback from both the stakeholders and the technical staff.
- Validation of the migration process for existing applications on the Cloud that public authorities want to utilise.

Cloud migration of public services is not a process visible to citizens; therefore, validation of the migration process might be limited. However, leadership from top management within the organization is essential. Technical people in charge of migration will have to consider political cycles and be prepared for changes in the management structure. There may be internal personnel in the city authorities who are reluctant to change. Therefore change management policies must be foreseen and put into practice from the very beginning. These actions may require training activities for personnel to adapt their competencies to a new IT environment. In order to monitor from a technical point of view, one has to consider the following aspects:

- Before going into a migration process, it is imperative to check that all documentation for the applications is available. If this is not the case, the impact must be evaluated.

It is particularly important to have a detailed technical plan to ensure that all the required elements will be available prior to migration. This refers to aspects such as source code, documentation, availability of technical support -whether internal or external- similarities/differences between the existing IT environment and the Cloud environment and ways to cope with these differences (e.g. OS versions), etc.

- The availability of trained personnel for the new environment needs to be ensured, either by training existing technical people or by hiring new personnel.
- The ownership of applications to be migrated must be ensured before the process is to start. Existing applications may be locked in by legal agreements with vendors.
- Security and data privacy are a serious concern. Technical staff must ensure these points and effectively communicate them to management.

3.4 Conclusions and Discussion

The guidelines analysed in the previous section allow city authorities to take full advantage of the cloud computing paradigm, providing innovative and highly reliable services to their citizens, despite any resource constraints. Today, the majority of existing cloud offerings are implemented in proprietary and highly standardized form, not only creating vendor lock-in, but also creating limitations to fully reaping the benefits of cloud computing. Systems composed of *open technologies* provide the freedom to change environments and deliver a robust and secure experience, extending existing IT to the cloud. Experience from experimentation in the four pilot cities has made it clear that embracing an open cloud should be done by using widely accepted open source technologies in all components of the platform and any micro-service endpoints, such as OpenStack, Cloud Foundry, Docker, LAMP for the implementation of applications' VMs, MySQL for database services, HAProxy for load balancing, Zabbix for monitoring, etc. The adoption of open source technologies means that benefits will be created without significant development effort; while new, emerging standards will also increase the portability and interoperability of systems across Cloud Service Providers, and will reduce or eliminate this current barrier to cloud adoption.

This idea of openness does not only refer to the adoption of open technologies but also to other components of a city's smart city strategic vision, creating externalities to all aspects of the innovation ecosystem. This means that city authorities should focus on adopting an *open innovation methodology* aiming to gather external and internal knowledge to accelerate the process of innovation. As the role of government has shifted over recent years from managing and administering to the orchestration of open innovation processes, stakeholders have become key players in deciding on, contributing to and delivering services (The World Bank 2015). Such a development has not only removed the entire burden from public authorities to a wider group of actors, but has also increased openness, transparency and inclusiveness. Thinking about public online services, means to improve the organization of public administration and to facilitate communication between public authorities and citizens. As public services have multiple stakeholders, each one deriving some value (Hartman et al. 2010), their engagement is an integral part of the success in any migration strategy. Even for a very technical task, such as migration of a public service to the Cloud, stakeholders' involvement strengthens public awareness with regards to the efforts made by the public authorities to modernise themselves. Experience from the STORM Clouds project has shown that cloud migration should be an open innovation activity, at the end of the day though, it is important to focus on 'quality', i.e. the involvement and true commitment of a limited number of stakeholders, rather than 'quantity'.

While moving to the Cloud environment, the decisions that city authorities have to make are complex and in many cases constitute a deterring factor for Cloud adoption. Deployment model, service category, and Cloud provider can create an overwhelming situation that requires technical, legal, financial decisions to be made. As already explained in the roadmap, out of the three cloud service categories IaaS might be the most flexible solution for authorities that want to use their own applications. However, it depends on cloud platform administrators when it comes to configuring all the components for scalability and high availability. Experimentation in the four STORM Clouds project cities provided a two-model solution that offers high availability and scalability features, coupled with high transparency to application owners. More specifically, by accompanying the IaaS layer with the Data Service layer and Access layer, the data and the HTTP traffic management are delegated to the platform; while the application's business logic is still contained on the VM(s). This approach offers great flexibility as it does not require architectural changes to the applications but also keeps the deployment complexity low because the application owner "leverages" the high availability and scalability features of the platform (Battarra et al. 2016). When selecting the service cloud provider, as previously mentioned, an OpenStack based service provider was used. Open Stack Foundation maintains a marketplace that helps public authorities make informed decisions, while also carrying out interoperability testing to validate OpenStack powered products. Other criteria for the selection of the provider were the location of the infrastructure as well the offering of a monthly calculator that allows public authorities to evaluate different hosting options and the operation of alternative architectures.

Once these initial decisions are taken, city authorities move on to the migration process, which -for most- is more of a trial and error phase without careful prior planning. In the STORM Clouds project, we generated evidence that for a successful redeployment of applications to the Cloud environment, city authorities have to design a comprehensive plan and to automate the migration process. Automation, which is encouraged in the case of the cloud as it is a programmable infrastructure, can be achieved through the use of a set of tools and procedures. In the four pilot cities, participating in the project, automation was achieved with the use of Open Stack Heat, in two steps: first in order to prepare the bash shell scripts that configure the VM hosting the applications and install and configure the application and its dependencies, and second for creating the Heat scripts that describe the architecture of the applications and integrate them with the installation and configuration scripts. Automation also allows other interested cities to select and deploy applications through a cloud-based services portfolio.

Cloud computing is a disruptive innovation that is expected to bring a new wave of benefits over the coming years. Apart from being a catalyst in terms of technology, it is also expected to create new business models and ways of collaboration allowing SMEs, but also non-IT companies and organizations to capitalise on the Cloud (Hobson 2014). Actually, it divides the role of service providers into two: the infrastructure provider, who manages a cloud platform and leases resources according to a usage-based pricing model; and the service provider, who rents such resources to serve the end-users (Zhang et al. 2010). Based on this and the principles of open innovation, cloud computing allows the selection and re-use/replication of software applications, targeting common urban challenges from software repositories or other online smart city platforms. This allows the uptake of a large number of smart city applications by standardising and simplifying their customisation and use.

References

Angelidou, M., Psaltoglou, A., Komninos, N., Kakderi, C., Tsarchopoulos, P., & Panori, A. (2017). Enhancing sustainable urban development through smart city applications. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/JSTPM-05-2017-0016.

Australian Government (2011). Cloud computing strategic direction paper: opportunities and applicability for use by the Australian Government. Department of Finance and Deregulation. https://www.finance.gov.au/files/2013/04/final-_cloud_computing_strategy_version_1.1.pdf. Accessed 3 April 2017.

Battarra, M., Consonni, M., Domenico, S., & Milani, A. (2016). Storm clouds platform: a cloud computing platform for smart city applications. *Journal of Smart Cities, 2*(1), 14–25.

Bonneau, V., Mahieu, B., Dudenbostel, T., Gaudemer, J., Giarracca, F., Good, B., Poel, M., Ramahandry, T., & Van Til, J. (2013). Analysis of cloud best practices and pilots for the public sector. Study prepared for the European Commission DG Communications Networks, Content and Technology, Digiworld by IDATE and Technopolis [group]. http://www.storm-clouds.eu/services/2017/04/analysis-of-cloud-best-practices-and-pilots-for-the-public-sector/. https://doi.org/10.2759/35653.

Brophy, T. (2016). 7 Cloud migration considerations. *Network Computing*. Retrieved March 31, 2017, from https://www.networkcomputing.com/cloud-infrastructure/7-cloud-migration-considerations/1926792235.

Chandrasekaran, A., & Kapoor, M. (2011). State of cloud computing in the public sector—a strategic analysis of the business case and overview of initiatives across Asia Pacific. Frost & Sullivan Global Growth Consulting Company. Retrieved March 28, 2017, from https://www.frost.com/sublib/display-market-insight.do?id=232651031.

Cloud Security Alliance (CSA) (2016). *A repeatable cloud-first deployment process model*. Retrieved March 22, 2017, from https://cloudsecurityalliance.org/download/a-repeatable-cloud-first-deployment-process-model/.

Cloud Standards Customer Council (CSCC). (2018). Migrating applications to public cloud services: roadmap for success. Retrieved April 26, 2017, from http://www.cloud-council.org/deliverables/CSCC-Migrating-Applications-to-Public-Cloud-Services-Roadmap-for-Success.pdf.

Craig, R., Frazier, J., Jacknis, N., Murphy, S., Purcell, C., Spencer, P., & Stanley, J. D. (2009). *Cloud computing in the public sector: public manager's guide to evaluation and adopting cloud computing*. White Paper, Cisco Internet Business Solutions Group. Retrieved April 30, 2017, from https://www.cisco.com/c/dam/en_us/about/ac79/docs/wp/ps/Cloud_Computing_112309_FINAL.pdf.

Deloitte (2011). Study on cloud and service oriented architectures for e-government. Final report summary, Commissioned by the European Union. Retrieved March 31, 2017, from https://ec.europa.eu/digital-single-market/en/news/study-cloud-and-service-oriented-architectures-e-government-smart-2010-0074-%E2%80%93-final-report.

Díaz-Díaz, R., Muñoz, L. & Pérez-González, D. (2017). The business model evaluation tool for smart cities: application to SmartSantander Use Cases. *Energies*, *10*, 262, 1–30. https://doi.org/10.3390/en10030262.

Environmental Protection Agency (EPA) (2017). *EPA hosting readiness assessment process*. Retrieved March 31, 2017, from https://developer.epa.gov/guide/wp-content/uploads/sites/3/2016/04/conops_epa_cloud_readiness_508_092116.pdf.

European Cloud Partnership Steering Board (ECPSB) (2014). Establishing a trusted cloud Europe: a policy vision document by the Steering Board of the european cloud partnership. Final report prepared for the European Commission. *DG Communication Networks, Content & Technology*. https://www.kowi.de/Portaldata/2/Resources/horizon2020/coop/Report-Establishing-trusted-cloud-Europe.pdf. Accessed 26 March 2017.

European Commission (EC) (2012). Unleashing the Potential of Cloud Computing in Europe, Brussels, 27.9.2012, COM(2012) 529 final.

European Commission (EC) (2014). Towards a Cloud of Public Services. Digital Agenda for Europe. Retrieved March 26, 2017, from https://ec.europa.eu/digital-single-market/en/news/towards-cloud-public-services-0.

Frost & Sullivan (2011). *Tips for choosing a cloud service provider*. Retrieved March 23, 2017, from https://ibm.co/2plUvkr.

Giannakoulias, A. (2016). Cloud computing security: protecting cloud-based smart city applications. *Journal of Smart Cities*, *2*(1), 66–77. https://doi.org/10.18063/jsc.2016.01.007.

Hamilton, S., & Zhu, X. (2017). Funding and financing smart cities. Deloitte Center for Government Insights. Deloitte Development LLC. Retrieved March 24, 2017, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-ps-funding-and-financing-smart-cities.pdf.

Hobson, L. (2014). Major disruption—cloud computing is disrupting more than our technological norms. Retrieved March 21, 2017, from https://www.linkedin.com/pulse/20141006134234-1064759-major-disruption-cloud-computing-is-disrupting-more-than-our-technological-norms.

Information Commissioner's Office (ICO) (2014). Conducting privacy impact assessments: Code of practice. Data Protection Act. Retrieved May 3, 2017, from https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

IDC (2012). Quantitative estimates on the demand for cloud computing in Europe and the likely barriers to up take. Smart 2011/0045, D4 Final Report, Contract Nr 30-CE-0439644/00-29. Retrieved March 27, 2017, from https://ec.europa.eu/digital-single-market/en/news/quantitative-estimates-demand-cloud-computing-europe-and-likely-barriers-take-final-report.

Kakderi, C., Komninos, N., & Tsarchopoulos, P. (2016a). Smart cities and cloud computing: introduction to the special issue. *Journal of Smart Cities, 2*(1), 1–3.

Kakderi, C., Komninos, N., & Tsarchopoulos, P. (2016b). Smart cities and cloud computing: Lessons from the STORM CLOUDS experiment. *Journal of Smart Cities, 2*(1), 4–13.

Komninos, N. (2015). *The age of intelligent cities*. New York: Routledge.

Komninos, N., Bratsas, C., Kakderi, C., & Tsarchopoulos, P. (2016). Smart city ontologies: improving the effectiveness of smart city applications. *Journal of Smart Cities, 1*(1), 31–46.

Komninos, N., Tsarchopoulos, P., & Kakderi, C. (2014). New services design for smart cities: a planning roadmap for user-driven innovation. In *Proceedings of the 2014 ACM International Workshop on Wireless and Mobile Technologies for Smart Cities (WiMobCity '14)* (pp. 29–38), Philadelphia, Pennsylvania, USA: ACM. https://doi.org/10.1145/2633661.2633664.

Komninos, N., Pallot, M., & Schaffers, H. (2012). Special issue on smart cities and the future internet in Europe. *Journal of the Knowledge Economy, 4*(2), 119–134.

KPMG (2012). Exploring the cloud: A global study of governments' adoption of cloud. KPMG International Cooperative. Retrieved March 7, 2017, from https://images.forbes.com/forbesinsights/StudyPDFs/exploring-cloud.pdf.

Mahmood, Z. (2016). *Cloud computing technologies for connected government*. Hershey PA: Information Science Reference. ISBN 978-1-4666-8629-8.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800–145, U.S. Department of Commerce. Retrieved March 9, 2017, from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.

Miller, P., Matzke, P., Glenn, M., & Neuburg, S. (2018). Taking the pulse of Europe's cloud: What CIOs need to know about cloud in Europe as we enter 2018, Forrester research. https://www.forrester.com/report/Taking+The+Pulse+Of+Europes+Cloud/-/E-RES132012. Accessed 9 March 2017.

Mora, L., Bolici, R., & Deakin, M. (2017). The first two decades of smart-city research: a bibliometric analysis. *Journal of Urban Technology*, *24*(1), 3–27 (2017). https://doi.org/10.1080/10630732.2017.1285123

Panori, A., González-Quel, A., Tavares, M., Simitopoulos, D. & Arroyo, J. (2016). Migration of applications to the cloud: a user-driven approach. *Journal of Smart Cities*, *2*(1), 41–52 (2016). https://doi.org/10.18063/jsc.2016.01.005.

Pelerin, R. (2015). Testing key to successful cloud migration, DataCentreKnowledge. Retrieved March 4, 2017, from http://www.datacenterknowledge.com/archives/2015/04/29/testing-key-successful-cloud-migration/.

Posey, B. (2015). Criteria for choosing a public cloud provider. http://bit.ly/1QeOlHm. Accessed 4 March 2017.

Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., & Oliveira, A. (2011). Smart cities and the future internet: Towards cooperation frameworks for open innovation. In: J. Domingue et al. (Eds.), *The future internet* (pp. 431–446). FIA 2011. Lecture Notes in Computer Science, Vol. 6656. Springer, Berlin, Heidelberg, ISBN 978-3-642-20897-3. https://doi.org/10.1007/978-3-642-20898-0_31.

Seo, J., Min, J. & Lee, H. (2014). Implementation strategy for a public service based on cloud computing at the government. *International Journal of Software Engineering and its Applications*, *8*(9), 207–220 (2014). https://doi.org/10.14257/ijseia.2014.8.9.17.

Tsarchopoulos, P., Komninos, N., & Kakderi, C. (2017). Accelerating the uptake of smart city applications through cloud computing. *World Academy of Science, Engineering and Technology, International Journal of Social, Behavioural, Educational, Economic, Business and Industrial Engineering, 11*(1), 129–138.

VMware (2011). Your Cloud in the Public Sector. Industry Brief White Paper.

West, M. D. (2010). Steps to improve cloud computing in the public sector. *Issues in Technology Innovation, 1,* 1–13.

Writer, S. (2013). A reference model for moving your applications to cloud. Retrieved March 31, 2017, from https://www.ibm.com/blogs/cloud-computing/2013/08/a-reference-model-for-moving-your-applications-to-cloud/.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), 7–18.