OECD Digital Economy Papers No. 240

Cloud Computing: The Concept, Impacts and the Role of Government Policy

OECD

https://dx.doi.org/10.1787/5jxzf4lcc7f5-en

OECD

Unclassified **DSTI/ICCP(2011)19/FINAL**

Organisation de Coopération et de Développement Économiques
Organisation for Economic Co-operation and Development **19-Aug-2014**

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON DIGITAL ECONOMY POLICY

DSTI/ICCP(2011)19/FINAL
Unclassified

CLOUD COMPUTING: THE CONCEPT, IMPACTS AND THE ROLE OF GOVERNMENT POLICY

JT03361226

Complete document available on OLIS in its original format

English - Or. English

FOREWORD

This report on *Cloud Computing: The Concept, Impacts and the Role of Government Policy* was discussed and approved for declassification by the Committee on Digital Economy Policy (CDEP, former Committee for Information, Computer and Communications Policy) in October 2012. It was drafted by Ms. Verena Weber under the guidance of Ms. Anne Carblanc, both of the OECD's Directorate for Science, Technology and Industry (DSTI).

TABLE OF CONTENTS

CLOUD COMPUTING: THE CONCEPT, IMPACTS AND THE ROLE OF GOVERNMENT POLICY

Main points

Cloud computing is changing the way computing is undertaken. Users of cloud computing infrastructure and services do not have to make upfront, capital-intensive investments in information technology (IT) infrastructure and software but, instead, can pay for computing resources in a pay-as-you go model. Cloud computing providers have significantly lower operating costs than companies would have if they ran their own IT infrastructure, due to their global scale and the possibility to aggregate the demand of multiple users of cloud computing, especially in 'public clouds'. They are able to provision computing resources in a rapid and elastic way, allowing adjustment to changing requirements.

From an economic perspective, cloud computing provides the ability to access IT resources on demand without the need for significant capital expenditure. It thereby significantly lowers the entry barriers for new entrants in multiple sectors. Cloud computing has thus the potential to *become a veritable platform for innovation that spurs the development of new products and services.* In the context of innovation, cloud computing also facilitates online collaboration on a global scale. In addition, it is particularly interesting for small- and medium-sized enterprises (SMEs) that are an important source of economic growth, job creation and innovation in many OECD member countries. By leveraging cloud computing solutions, SMEs save on investment costs and at the same time, benefit from gaining access to cutting edge technology and services, including software updates. Large companies, institutions and governments are examining cloud computing as an important cost saving option to reduce expenditures on IT infrastructure and services and ongoing maintenance costs. Overall, cloud computing is expected to have a *positive impact on economic growth*. It is further expected to have *positive environmental impacts* due to its carbon abatement potential.

However, the term cloud computing is currently often used as a marketing term and multiple definitions of cloud computing exist. As such, the concept is still "cloudy". This report defines cloud computing as "*as a service model for computing services based on a set of computing resources that can be accessed in a flexible, elastic, on-demand way with low management effort*." Furthermore, it emphasises that the concept covers a whole cloud service spectrum consisting of infrastructure as a service, platform as a service and software as a service, as well as multiple delivery models including private, public, hybrid and community clouds.

The benefits of cloud computing mentioned above, however, are accompanied by challenges and open issues. Challenges in the area of privacy - including cross-border issues related to privacy protection - need to be addressed (see below). In addition, in the area of security, it is essential to assess and manage risk in a thorough and holistic manner since cloud computing is becoming a crucial element of networked computing. While such risk management may be feasible for multinationals, it may be difficult for SMEs or consumers. Furthermore, there are issues regarding the liability of service providers in current terms and conditions of standard cloud computing contracts. An additional major open issue is the current lack of open standards, especially in the area of platform as a service. Finally, cloud computing as an on-demand service offering may also have structural implications for the IT sector which could benefit from further economic analyses.[1]

Given the positive economic impact of cloud computing, but also the challenges inherent to cloud computing, *policy makers* have an important role to play in a *multitude of areas*:

- **Spurring the use of cloud computing**. Governments have a role to play in further spurring the use of cloud computing, for instance, through removing unnecessary legal and regulatory barriers, being lead users, through fostering skills and education, through supporting R&D projects and establishing public-private partnerships.

- **Standards.** One of the major challenges facing the development of cloud computing is the lack of appropriate standards in some areas, the lack of widespread adoption of existing standards and the potential for vendor lock-in due to the use of non-interoperable solutions. Governments should encourage and support the continued development of open interoperable standards for business support, provisioning and configuration by, for example, coordinating with different standards institutes or by mandating open standards in public procurement.

- **Measurement of cloud computing**. To date, there is little publicly available data in the area of cloud computing. Policy makers, in consultation with stakeholders, could play a role in identifying relevant criteria and developing a standard framework for the measurement of cloud computing.

- **Cloud computing for development**. Cloud computing provides a very interesting means for organisations and consumers in developing countries to access powerful computing resources at low cost. However, some challenges must be overcome to allow this to happen, such as ensuring the availability of broadband network infrastructure. Policy makers have an important role to play in: *i)* expanding fixed and wireless broadband access in developing countries; and *ii)* spurring the development of cloud computing and the adaptation of cloud services in these countries to take advantage of cloud computing resources to spur economic growth, enhance educational capabilities, provide online tools for open government, and enable the free flow of information for overall societal development.

- **Broadband infrastructure**. With the growth of cloud computing, the demand for bandwidth is expected to increase significantly. Policy makers should take steps to help accelerate broadband infrastructure deployment, including by freeing up additional spectrum for mobile broadband. They should promote the most flexible network technologies and topologies and spur competition so that reliable solutions that promote the most bandwidths can develop.

- **Trade and competition implications**. It may still be too early to evaluate the trade and competition implications of cloud computing. However, policy makers should keep in mind the possibility that anti-competitive practices result from market domination by a few companies in the future and avoid harmful barriers to competition. They should also keep in mind the relationship between the efficient flow of data across jurisdictions and the growth of cloud computing.

- **Tax implications**. As more companies move to the cloud, including companies with potentially less experience in cross-border transactions and accounting, policy makers will need to consider the tax implications. These are foreseen as being mainly related to record keeping requirements and possible evasion of taxes.

- **Contractual issues**. Standard cloud computing contracts can present some challenges. Standard contracts between service providers and SMEs and consumers are often non-negotiable and offer “take-it-or-leave-it” terms. The details of the contract terms may not be well understood by novice users with limited legal expertise or the terms may not provide the expected legal coverage for providers in certain jurisdictions, resulting in risk and uncertainty for both providers and users that could inhibit the growth of cloud computing. Additionally, service level agreements should better address service outages and provide concrete remedies should an outage occur. Policy makers could urge the development of industry codes-of-conduct and improved delivery methods (e.g. video) for standard, non-negotiable contracts.

- **Security and risk management**. Cloud computing leverages many forms of existing hardware and software technology and the OECD Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security (OECD, 2002) provide a relevant approach to deal with, if not all, at least several cloud computing security challenges. Four of its principles should be applied in particular: *i)* Risk assessment, *ii)* security management, *iii)* security design and implementation, and *iv)* risk reassessment. In addition, authentication and identity management challenges need to be addressed as individuals conduct more of their online activities through cloud-based services.

- **Privacy.** In the area of privacy, a globally interoperable approach by governments would facilitate the deployment of cloud computing. More particularly, policy makers should address the questions of whose laws apply to the data stored in the cloud, including who can access this data, and under which circumstances processing of data in the cloud amounts to a cross-border transfer.

Due to its potential impact on economic growth but also in light of the challenges raised by cloud computing, it is proposed to continue work in this area. Main proposals for continued work include privacy and other jurisdictional issues such as liability and compliance, security, cloud computing contracts, impact assessment, the structural changes within the IT sector and companies' IT departments as well as cloud computing for development.

Introduction

The cloud has been changing the way computing is undertaken. Users of cloud computing infrastructure and services do not have to make upfront, capital-intensive investments in Information Technology (IT) infrastructure and software any more but, instead, can pay for computing resources in a pay-as-you go model. Computing is thus deemed to become a utility. This trend is particularly interesting for small and medium enterprises (SMEs), including start-ups, as it allows immediate, on-demand access to information technology resources without the need for capital expenses in hardware and software and thus significantly decreases entry barriers. In addition, many large companies, institutions and governments are examining cloud computing as an important cost saving option that can reduce expenditures on IT infrastructure and services and ongoing maintenance costs.

Cloud computing is rapidly accelerating the amount of data that is transferred and stored across borders, thereby highlighting a number of issues in areas such as data security, privacy (including cross-border issues linked with privacy protection), interoperability and data portability as well as the availability of service. Cloud computing may also have structural implications for the IT sector and is viewed by some as having positive environmental benefits since new server farms have the potential to process data in a very efficient manner and hence it can help decrease over-provisioning of IT infrastructure at the business and government level.

Because of the important potential of cloud computing for economic and social development, the present analysis is developed in the context of the work of the Committee on Digital Economy Policy (CDEP, former Committee for Information, Computer and Communications Policy) on the Future of the Internet Economy (item 1.7 of the Committee's Programme of Work and Budget 2011-2012). The work builds on the CDEP's Technology Foresight Forum held in October 2009.

The main objectives of the report are to:

- present the concept of cloud computing, the services it provides and deployment models, and thus give a clear overview of what it is and what it is not.
- provide an overview of how cloud computing changes the way computing is carried out.
- evaluate the impacts of cloud computing (including its benefits and challenges as well as its economic and environmental impacts).
- discuss the policy issues raised by cloud computing and the role of governments and other stakeholders in addressing these issues.

Cloud computing: Definitions, characteristics, service models and deployment

Cloud computing has become the IT focus of many companies, and is leading many IT companies to brand their offerings as cloud computing services. Consequently, multiple definitions and interpretations of cloud computing have emerged. This section provides an overview of selected definitions and describes the main characteristics of cloud computing including an overview of cloud service and deployment models.

Definitions and characteristics of cloud computing

One of the reasons why multiple definitions of cloud computing exist is that cloud computing does not refer to a specific technology but rather to a concept comprising a set of combined technologies (Schubert et al., 2010).

Two definitions which both evolved after extensive brainstorming and multi-stakeholder consultation describe the core aspects of this concept in a comprehensive way: The definition by the US National Institute of Standards and Technology (NIST, 2011) and the definition by the Berkeley RAD lab (Armbrust et al., 2009) (see Table 1).

Table 1. Selected definitions of cloud computing

Institution	Definition
US National Institute of Standards and Technology (NIST)	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.
Berkeley RAD Lab	Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS), so we use that term. The datacenter hardware and software is what we will call the cloud.

Source: Armbrust et al. (2009), NIST (2011)

The first definition focuses more on the purpose of cloud computing, the latter concentrates more on the components of cloud computing. They show that cloud computing can be understood *as a service model for computing services based on a set of computing resources that can be accessed in a flexible, elastic, on-demand way with low management effort*.

The following *characteristics*, which are generally inherent to cloud computing, but not necessarily a feature of every cloud computing solution, shed further light on the concept. They include according to NIST (2011), Armbrust et al. (2009), and Schubert et al. (2010):

- *On-demand self servic*e: Users of clouds can "unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider" (NIST, 2011).

- *Availability of "infinite" computing resources:* Cloud users do not have to plan the provision of their computing resources in advance as they have the potential to access computing resources on demand.

- *Rapid elasticity and adaptability:* Elasticity is one of the key features of cloud computing. Computing resources can be provisioned in an elastic and rapid way that allows adaptation to changing requirements such as the amount of data supported by a service or the number of parallel users. Users can buy computing services at any time at various granularities. They are able to up- and downscale those services according to their needs.

- *Elimination of up-front commitment:* Users of cloud services do not have to make heavy, upfront IT investments allowing companies to start small and to successively increase hardware and software resources only when needed. In addition, small and medium enterprises have a much easier and more affordable access to state-of-the-art applications and platforms which were only available for larger companies before.

- *Short-term pay for use:* Users are able to pay for their use of cloud services on a short-time basis thereby only paying for the time they use the computing resources and release them when they do not need them anymore. Companies are thus able to reduce capital expenses (capex) and convert them into operating expenses (opex).

- *Network access:* Computer services are accessed over the network and through standard mechanisms which allow users to connect several devices to the cloud (e.g. laptops, mobile phones).

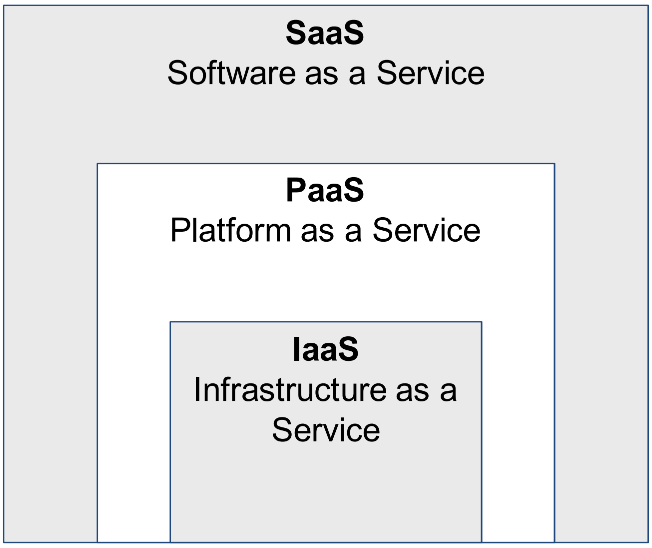
- *Pooling of resources:* Providers' cloud services "are pooled to serve multiple customers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand" (NIST, 2011). As a consequence, users of cloud computing usually do not know and are unable to control where the provided cloud computing resources are exactly located. It is, however, in certain cases possible to specify the location at a more abstract level (e.g. continent, country).

- *Measured service and adaptability:* Cloud computing systems are able to react on-time to changes in the amount of computing resources requested and thus automatically control and leverage resources.

*Everything as a Service (*aaS:) Cloud service and usage models*

As the definition by the Berkeley RAD Lab has shown, cloud computing covers a huge range of services including software, platform and infrastructure services. Accordingly, multiple and diverse cloud computing service models exist. They can be categorised into: *i)* software as a service (SaaS); *ii)* platform as a service (PaaS); and *iii)* infrastructure as a service (IaaS) (see Figure 1). In the next paragraphs, these service models are briefly discussed and some examples of current cloud services and cloud service providers are given for each type of service model.

Figure 1. Categories of cloud computing service models



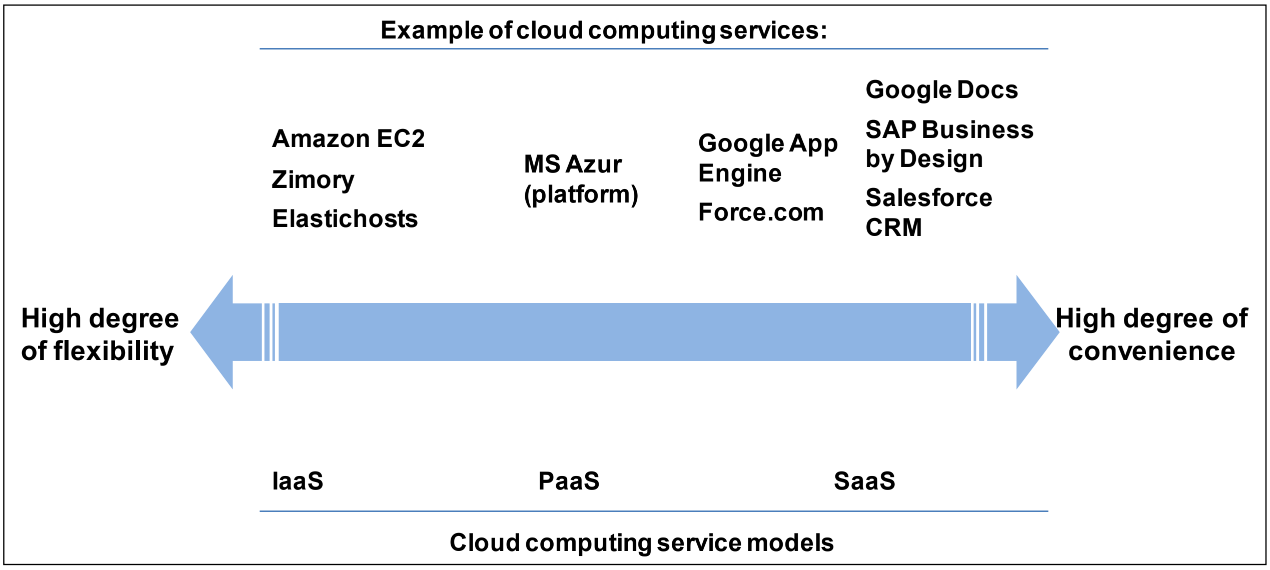
Infrastructure as a service (IaaS) provides computing resources such as processing, storage and networks to the users of clouds, and enables users to leverage these resources through their own implementation of virtualisation capabilities. Providers of these hardware virtual machines offer access to raw computing resources and a high degree of flexibility. IaaS users are able to access computational resources (e.g. CPUs), and run operating systems and software on the provided computing resources. The flexibility for users is very high is the IaaS model as there are only few limits on the kinds of application that can be hosted on these services. Examples of services that fall into the IaaS category include Amazon Elastic Cloud (EC) 2 and Zimory.

Platform as a service (PaaS) provides users a more structured platform to deploy their own applications and services. Typically, users rely on programming languages and further tools of the cloud provider to deploy these applications. Cloud users do not manage or control the underlying infrastructure such as networks or operating systems (NIST, 2011), with the service provider managing the virtualisation operations. Suppliers of PaaS use dedicated application programming interfaces (APIs). As each cloud provider generally relies on its own API, it is typically difficult to move applications from one cloud provider to the other. There are initial attempts, however, to develop generic programming models. Examples for PaaS include the Windows Azure Platform and the Google App Engine.

In the SaaS model, cloud users directly access the applications of the cloud provider and therefore have the convenience of not having to manage the underlying infrastructure or the capabilities of the applications (NIST, 2011). SaaS cloud services include applications for specific business processes and purposes. The spectrum of examples is large and ranges from e-mail applications used by consumers to business applications and integrated management software solutions such as customer relationship management (CRM) tools, document management or accounting solutions, to name just a few.

Overall, the variety of cloud services spans a wide spectrum; on the one hand, there are services providing a very high degree of flexibility and customisation while on the other hand, there are services providing a high level of convenience. Figure 2 shows this spectrum and provides selected concrete examples of services which can also be combined. Due to the difference in services, different benefits and challenges, including policy challenges, apply more to some service models than to others.

Figure 2. Overview of *cloud service models* and some representative examples of types of cloud services



Shaping the cloud: Different cloud deployment models

When referring to cloud computing, it is also helpful to define whether a cloud is deployed within an organisation or more broadly. Four main deployment models can be distinguished: *i)* private clouds, *ii)* public clouds *iii)* community clouds, and *iv)* hybrid clouds.

Private clouds, as their name indicates, refers to data centres that are typically owned or leased by one company with the underlying hardware, software and network infrastructure not shared with others. They can be located on the company's sites or off-site. *Public clouds*, in contrast, make the data centre publicly available or to a large industry group (NIST, 2011). Services in a public cloud are typically owned by a cloud service provider. *Community clouds* can be categorised into private or public community clouds (Schubert, Jefferey et. al., 2010). Private community clouds are shared by a community which has common concerns (e.g. smaller organisations or research institutes) and public community clouds are provided by cloud service resellers that bundle services of different cloud providers and resell them. Finally, *hybrid clouds* employ both private and public infrastructure such that a section of the data centre is reserved for a single tenant, and the remainder is available to the public. Hybrid clouds are typically employed when only part of the data is supposed to be outsourced in order to keep full control of sensitive data and, at the same time, take advantage of higher flexibility through outsourcing.

These different deployment models combined with the above mentioned service models present an almost endless variety of potential benefits, use cases, data elements, types of users and possible risks. While cloud computing services may be definable, as a range of common elements and concepts, actual deployments do not lend themselves to any one-size-fits-all model so that benefit and challenges depend on the concrete cloud computing model in use.

Benefits of cloud computing: Flexibility, cost efficiency, and a platform for innovation

Due to its inherent characteristics, cloud computing brings important benefits to organisations. One important dimension is the rapid elasticity of computing resources. Organisations can rapidly buy or relinquish computing resources according to their needs and do not have to perform costly and time-intensive upgrades of their infrastructure, nor do they have to plan the provision of those resources in advance where they have quasi-infinite access to computing resources in the cloud (see also Box 1).

Box 1. Case study: Netflix moving the Cloud

Over the past years, Netflix, an Internet subscription service for music and video streaming with over 25 million subscribers, moved many of its services to the cloud as the company realised that it could not build new datacenters fast enough for the growing demand. To illustrate this, the graph below shows the growth in requests for the Netflix API which allows Netflix's customers to build their own Netflix-integrated applications for the Internet, the desktop, mobile devices or the TV. In autumn 2010, the requests reached the datacenter capacity. According to the company, nearly 100% of their IT infrastructure is now in the cloud and all international products are cloud based.

The main reasons for moving to the cloud are as follows:

- faster
- scalable (avoiding more own datacenter capacity)
- available (higher robustness and availability than datacenter services
- productive (optimisation of agility of a large development team with automation and tools).

Sources: Netflix.com; developer.netflix.com/ ; www.slideshare.net/adrianco/netflix-in-the-cloud-2011

A further important benefit constitutes in a potential reduction of IT costs. On the user side, cost reductions by using cloud computing result from the fact that traditional corporate IT infrastructure is in most instances underutilised due to over-provisioning. This is because it is necessary to provide capacity to handle data peaks, future expected loads and to prepare for cases of unanticipated growth in demand (Perry, 2008). On the provider side, cost reductions are achieved via an increased efficiency of the data centres run by cloud computing providers (e.g. through economies-of-scale). Due to their global scale and the possibility to aggregate the demand of multiple users of cloud computing, especially in public clouds, providers have much lower operating costs than companies would have if they would run their own IT infrastructure (see also Kushida, et. al., 2011).

Another important benefit is the transfer of IT expenditures from capital expenditures (capex) to operating expenditures (opex) that has an important impact on companies' investment capacity, also in the medium and long run. Users of cloud services do not have to build up their own server infrastructure, nor do they have to invest important quantities of capital in IT infrastructure and software as in the past. Investments in IT infrastructure are thus reduced significantly. This notably means that entry barriers for start-ups are significantly lowered (see also the section on the economic impact of cloud computing). In the medium run, the business idea will thus become much more center-stage and the upfront capital investments will become less important. Cloud computing has thus the potential to *become a veritable platform for innovation that spurs the development of new products and services.* In addition, it is also particularly interesting for SMEs that are an important source of growth and innovation in many OECD member countries. They save on investment costs and benefit at the same time by having access to cutting edge technology and services including software updates.

In this context of innovation, cloud computing also facilitates online collaboration on a global base. In addition, it is expected to aid the transition towards mobile computing as cloud computing could become an important way in which mobile applications operate.

The economic impact of cloud computing

As discussed in the previous sections, cloud computing has a transformative impact and provides a broad range of benefits. In terms of financial implications, cloud computing is supposed to offer a set of financial benefits and to have a positive economic impact (Etro, 2010; Wyld, 2010). However, due to the variety of different implementations of cloud computing and the fact that the concept as a whole including the combination of different service and deployment models is rather new, there is significant uncertainty and wide variations in estimates exist. In addition, a number of assumptions have to be made to estimate the cost reduction potential (e.g. the share of data that will be outsourced to the cloud, the choice of cloud service and deployment models).

This section discusses initial attempts to quantify the economic impact of cloud computing. In particular, it looks at two different aspects: First, it focuses on potential cost savings on the user side and will attempt to illustrate these savings with a study that assesses cost savings by governments as cloud users. Secondly, it then takes a broader approach by assessing the impact of cloud computing on GDP growth and the impact on jobs in the European Union, mainly considering the impact of cloud computing in the private sector. Overall, cloud benefits can be considered as the direct benefits in use of cloud services such as increased efficiency and flexibility as well as the indirect benefits of new businesses that can exist because of the cloud environment.

The first study analyses the cost saving potential from government agencies moving to the cloud (West, 2010). It is based on the NIST definition of cloud computing discussed in the first section of this report. West's estimates are based on the assessment of several case studies of US government agencies that moved certain applications to remote file servers. They involve the US State Department, National Aeronautics and Space Administration, the Air Force as well as the cities of Los Angeles, CA, Washington, D.C., Carlsbad, CA, and Miami, FL (West, 2010, p. 4). Table 2 presents the main applications that government agencies moved to the cloud. The data moved to the cloud in these case studies were considered low-sensitivity data and applications low-risk cloud solutions. After a review of the case studies, West (2010) concludes that the cost saving potential for governments ranges from 25% and 50%. Consequently, he recommends that governments invest in cloud computing and clarify procurement rules to facilitate purchasing through cloud services.

Table 2. Overview of applications moved to the cloud

Case study	Application moved to the cloud
U.S. State Department's Nonproliferation and Disarmament Fund (NDF)	NDF contracted with SaaS provider for a new application that would provide detailed budget information from any Internet service around the world.
National Aeronautics and Space Administration (NASA)	NASA has pioneered a new cloud system known as Nebula used for mission support, public education, and data communications and storage
Air Force	The 45th Space Wing of Air Force reduced 60 physical servers to four physical servers running a cloud virtualisation solution.
City of Los Angeles	The city of Los Angeles moved e-mail services for its 30 000 employees onto cloud file servers.
City of Washington, D.C.	Washington, D.C. city government shifted many of its 38,000 employee e-mail services across 86 agencies to the cloud.
City of Carlsbad, California	The city of Carlsbad moved its 1,100 employees onto a cloud e-mail and web conferencing solution.
City of Miami, Florida	The city of Miami chose a PaaS cloud model for its service hosting and mapping technology (to track its 311 services to residents on potholes, illegal dumping, or missed garbage collection).

Source: OECD based on West (2010)

The second study takes a broader approach and conducts a simulation of the introduction and diffusion of cloud computing in the European Union[2] (Etro, 2010). It considers all three cloud computing service models (Saas, PaaS, IaaS). The study focuses on the impact of cloud computing on GDP growth, business creation and employment in the private sector in the short and medium term. It focuses on five aggregated sectors[3] for which detailed and comparable official EU statistics were available. It further considers two scenarios with different adoption rates of cloud computing. The first scenario models slow adoption of cloud computing that corresponds to a 1% reduction of fixed cost savings due to cloud computing. The second scenario of rapid adoption corresponds to a 5% reduction in fixed costs. The model neglects some positive effects such as the creation of new network effects and positive externalities due to energy savings as thus provides rather conservative estimates.

Table 3 shows the results for the two scenarios in the short (1 year) and medium (5 years) run. The results range from 0.05% EU GDP growth under a scenario of slow adoption in the short term to 0.3% GDP growth under a scenario of fast adoption in the medium run. This GDP growth is further expected to have direct and significant counterparts in the effects of employment and in the creation of SMEs.

Table 3. Impact of cloud computing on GDP growth

	Short run (1 year)		Medium run (5 years)	
	Slow adoption (scenario1)	Fast adoption (scenario 2)	Slow adoption (scenario1)	Fast adoption (scenario 2)
GDP growth	**0.05**	**0.15**	**0.1**	**0.3**

Source: OECD based on Etro (2009)

In terms of employment, the author found that the introduction of cloud computing in Europe could lead to about an additional one million jobs in Europe as well as a reduction of the unemployment rate of around 0.5% to 0.6% in the short run and 0.2% to 3% in the long run. However, the author also notes that these estimates should be taken with care as the simulation estimates the impact on hours worked and as the effective impact depends on a number of institutional and structural features of the labour markets and their regulations.

In addition, the author focuses on the effect that overall fixed cost reductions induced by cloud computing has on the creation of new businesses and new entrants to market and their effects on the labour markets.[4] The study does not look at the number of jobs that cloud computing providers create, nor does it take the potential negative effects on jobs into account that could occur through the fact that organizations, as they move their IT infrastructure to the cloud, could potentially save labour as they do not have to maintain or update their systems any more or as traditional IT roles within organisations (e.g. storage, network administration) might disappear.

Overall, at this stage, there is still a lack of data to thoroughly assess the economic impact of cloud computing on the economies of OECD member countries and there is a need for more studies on the economic impact of cloud computing. One of the main challenges is that data on the different cloud services is currently not available and not even retrievable from annual reports of cloud computing providers. To fully estimate the economic impact, more data from the private sector and co-operation between the private and public sector is needed.

The environmental impact of cloud computing

Cloud computing can both have positive and negative impacts on the environment. In terms of positive impacts, large and relatively new server farms of cloud service providers have the potential to process data in a highly energy-efficient manner. Furthermore, over-provisioning of IT infrastructure can be avoided at the business and government level. On the cloud supplier side, however, negative impacts also occur. Building-up and maintaining cloud infrastructure adds, in a first step, to pre-existing IT infrastructure owned by businesses, governments and users. Furthermore, higher energy efficiency reduces costs and thus frees capital for further investments into new resources which may lead to rebound effects.[5]

An area where some research has already been published is the overall effect of cloud computing on carbon emissions. Table 4 gives an overview of the main positive and negative effects that will reduce or create CO_2e[6] emissions. Negative effects can be categorised into direct emission effects and primary and secondary rebound effects. The first effects arise, for example, through cloud computing material production, the use of cloud computing services and the disposal of cloud computing infrastructure. Regarding rebound effects, a distinction has to be made between primary and secondary rebound effects. Primary rebound effects arise directly through the fact that cost savings are used to expand the cloud services market to new customers or to invest it in additional infrastructure. Secondary rebound effects can be perceived as indirect rebound effects. Examples include an increased production and use of handheld devices such as smartphones or notebooks or the reuse of servers that have been switched-off and that are then seen as spare IT capacity.

Table 4. Overview of main positive and negative effects of cloud computing on CO_2e emissions

	Effects of cloud computing on CO_2e emissions	Effects taken into account in Thomond et al (2011)
	Negative effects of cloud computing	
Direct emission effects	Cloud computing material acquisition, production, distribution and disposal	Yes
	Carbon emissions created via the use of cloud computing	Yes
	Added cloud infrastructure to already existing IT infrastructure	No (only replace-ments considered)
Primary rebound effects	Increased energy consumption as cost savings are used to open existing cloud applications to new users	No
	Increased energy consumption as cash savings are reallocated to provide new cloud applications	No
	Increased energy consumption as cash savings are reallocated to increase other carbon emitting processes such as manufacturing	No
	Increased energy consumption as reduced cost barriers to cloud-based applications increases SME-demand	No
	Increased materials	No
	Increased travel and shipment	No
Secondary rebound effects	Increased use of goods and vehicles (including an increased use of devices such as smartphones connected to the cloud)	No
	Increased production of goods and vehicles (including increased production of devices such smartphones and notebooks)	No
	Increased use of infrastructure (including the use of switched-off servers for other purposes and increased energy consumption by handheld devices)	No
	Positive effects of cloud computing	
Primary effects	Reduced energy consumption through enhanced efficiency	Yes
	Reduced or eliminated materials	No (later)
	Reduced travel/shipment (e.g. reduced transportation of CDs or DVDs containing data that is digitally available in the cloud	No (later)
Secondary effects	Avoidance of over-provisioning of IT infrastructure	No
	Positive effects through an increased scale of cloud computing adoption (including less travels to work because information needed can be accessed anywhere; energy savings through more and more on-premise servers being switched-off)	No (partially later)
	Eliminated production of goods and vehicles (including reduced production of servers, reduced manufacturing facilities for CDs, DVDs etc. and packaging)	No
	Eliminated production and reduced use of infrastructure (including reduced use of server room cooling systems, reduced use of road infrastructure)	No

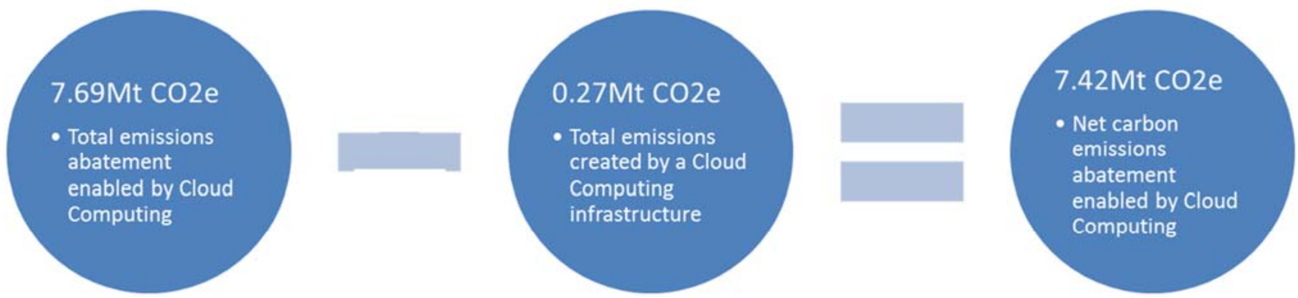
Source: OECD based on Thomond et al (2011)

Positive effects include primary and secondary effects. Examples of primary effects are reduced energy consumption through the use of efficient data centres for cloud computing as well as reduced or eliminated materials. Secondary effects include indirect effects provoked by an increased scale of cloud computing enabling additional teleworking capabilities, thereby reducing travel to work as well as a reduced use of infrastructure and the decommissioning of less efficient infrastructure.

Currently, research is underway aiming at quantifying these positive and negative effects and calculating the overall net effect. Thomond et. al. (2011) have developed a methodology for these effects and have come up with early results for the EU27 area. In terms of considered cloud services, the study focuses on a specific and narrower set of cloud computing applications mainly in the area of SaaS: e-mail, customer relationship management (CRM) and groupware. Regarding geographical coverage, the authors use aggregated EU27 level data as well as country-level data for seven European Union countries[7] to understand differences within the area. Finally, the authors assume that 80% of the organisations that are currently using on-premise servers for e-mail, CRM and groupware could shift to equivalent cloud services[8].

In terms of considered effects, Thomond et. al. (2011) focus on primary effects (see column 3 of Table 4) and on the fact that cloud computing will only enable carbon emissions abatement if less-efficient traditional on-premise severs are replaced by more efficient cloud servers. The estimations thus only capture a part of the cloud computing market and a part of the overall effects, but they allow to provide a first estimation of the carbon abatement potential of cloud computing. Overall, the authors estimate a total annual carbon abatement potential of 7.42Mt CO_2e (see Figure 3). This represents about 4% of the current carbon footprint of the ICT sector in the European Union or about "the permanent removal of nearly 2 500 000 cars" (Thomond et al, 2011, p. 9). Although the numbers are based on rather conservative assumptions, the overall carbon abatement potential is significant.

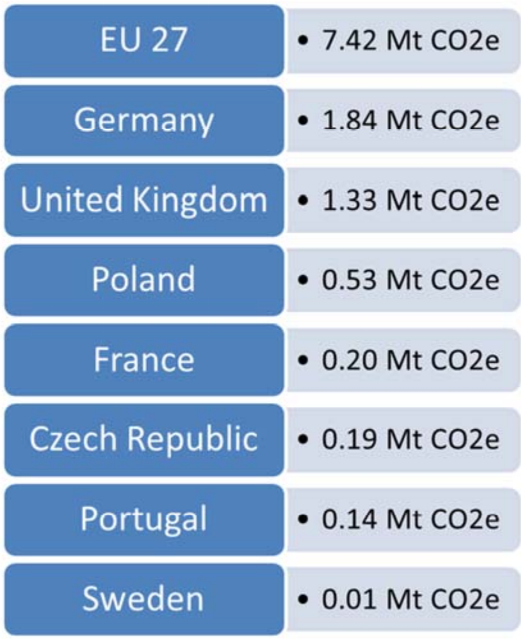
Figure 3. Potential annual carbon abatement enabled by cloud computing



Source: OECD based on Thomond et al (2011).

Regarding the abatement potential on the country level, the potentials differ a lot from one country to another (see Figure 4). The abatement potentials are low for France and Sweden since these countries consume less carbon intensive energy than other EU countries. Among the seven countries analysed, the United Kingdom and Germany have the largest abatement potential. A final interesting finding of the report is that 60% of the saving potential results from small and micro-sized organisations.[9]

Figure 4. The cloud computing abatement potential for EU 27 and on a country level



Source: OECD based on Thomond et al (2011).

Challenges and outstanding issues

In parallel to bringing significant benefits, cloud computing also raises challenges, some of which have already been raised in the context of outsourcing services and hosted solutions. The following paragraphs give an overview of several major outstanding issues and challenges.

Loss of IT-control

If significant parts of the IT infrastructure and services are moved to the cloud, a loss of control occurs to a certain degree. Cloud providers have the technical control over, for example, updates or new releases of software. Depending on the business model or implementation, they may decide whether or how they let users implement their own software and applications. To spur the deployment of cloud computing, however, cloud computing providers need to make sure to build trust so that customers have confidence in the cloud services offered. In addition, further issues are raised if data is moved to cross-border servers (see below).

Security and risk management in the cloud

As highlighted in the first section, cloud computing refers to a new concept but not to a specific, nor completely new technology. Cloud computing is rather characterised by a new scope and scale of networked computing, i.e. computing that is taken place in a fundamentally interconnected way. In 2002, the OECD adopted the *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Security Guidelines)* which include a set of principles that help address the challenges of computer security in a networked world. Therefore the Guidelines are particularly helpful to approach cloud computing security.

A key concept of the Security Guidelines is the recognition that static security measures are not effective in an open networked environment where the threats and the vulnerabilities are constantly evolving. Instead, the Guidelines promote a risk-based approach to security where risk is defined as the result of threats exploiting vulnerabilities and generating impact on business. To enhance security in an ever changing environment, security should result from a cycle including risk assessment, risk management and reassessment. In addition, security should be incorporated as an essential element of information systems and networks. According to this approach, cloud computing risks are highly contextual as the three components of risk vary as a function of many factors, such as the cloud service and deployment model in use, the nature of the cloud user (e.g. whether the user is a consumer, a SME or a multinational enterprise), and of the degree of criticality of the activity carried out in the cloud. Accordingly, it is important to identify and evaluate all key threats, vulnerabilities and their impact for the cloud service in use and the data involved. In addition, when assessing the risks of cloud computing services, it is always important to evaluate these risks against the risks carried by alternative scenarios.

Whereas the potential impact of the threats is highly contextual, vulnerabilities might, to a certain degree, be more characteristic of cloud computing. An Annex provides an illustrative overview of main vulnerabilities involved in cloud computing that have been reported in several studies (e.g. related to the availability of service)[10]. In addition, it presents the other side of the coin: the potential for cloud computing to diminish vulnerabilities – an aspect that is sometimes neglected.

None of these vulnerabilities is conceptually new and they all affect the classic security dimensions of confidentiality, integrity and availability of the data. However, some aspects of cloud computing exacerbate them, such as the outsourcing business model, the reliance on the Internet, the operation in a shared technical environment, the replication of data in different storage locations, etc. Vulnerabilities and benefits of cloud computing should be analysed in context and are only one parameter in a risk assessment, together with the analysis of threats and potential business impact. Risk assessment and the question of how to deal with risk are crucial. There are four options how the risk can be dealt with: it can be taken, terminated, managed or transferred. Risk management requires a holistic approach covering technological, human and organisational controls. Risk transfer can be undertaken by contractual solutions. However, there are some challenges in this area which are described in the section on cloud computing terms and conditions.

Finally, after deciding how to deal with the risk, it is essential to establish a continuous cycle of improvement whereby the effective and efficient implementation of security measures is appropriately overseen and audited, risks are regularly reassessed and where risk management controls are reviewed accordingly. In an open and dynamic environment such as the Internet, there is no such thing as a perfect state of security.

As was noted previously these security issues are not new in business-to-business environments, but the issues are less familiar to consumers and SMEs.

Privacy challenges in the cloud

The protection of personal data, i.e. "any information relating to an identified or identifiable individual ("data subject")" (OECD Privacy Guidelines, 1980), is also challenged in the cloud. Privacy issues for cloud service providers tend not to be cloud-specific, but rather draw from the broader set of privacy challenges posed by the Internet and by outsourcing arrangements. In the following, some examples of these issues are highlighted.

The first challenge results from the potential storage of data in multiple jurisdictions and their transfer from one jurisdiction to another for cloud resources management purposes. Often, the location of the jurisdiction of the server where the data is stored is not known to the cloud user, and as a result, the customer of cloud computing services, i.e. the main person responsible for the processing of data, may have difficulties to thoroughly check and control the data handling practices and to make sure that data is handled in a lawful way. There may need to be greater reliance on contractual solutions and alternative validations of processes and procedures. It should be noted that many of these issues already exist in outsourced situations, but may even be more complex in the cloud. In addition, in some cases personal data might even be held in or transferred to jurisdictions with unpredictable legal and regulatory frameworks which puts data protection at a high risk. Furthermore, the cloud user might not always be informed about data breaches. It has to be noted, however, that some cloud computing providers do detail their data handling practices and the geographical location of their data centres. Some offers also include certifications on data processing and data security procedures in use (ENISA, 2009).

Another legal issue concerns the question of who has a legal right, and under which circumstances, to access the data processed and stored in the cloud. This includes access to the data by government agencies for national security and law enforcement purposes, an issue which is particularly sensitive and would need to be addressed in an appropriate forum. Other legal challenges that OECD members could address include whose national laws apply to the personal data stored in the cloud given the multitude of differing national laws or which country is responsible for the arbitration of contract disputes i.e. the country in which the cloud computing service originated or the country in which the service is used (Zysman and Murray, 2011).

From a policy perspective, it is important to be aware of distinctions between different cloud business and use models. For example, some users of cloud services are organisations that are aware of the fact that they have to make important compliance efforts with respect to the protection of personal data. These organisations rely on cloud providers that charge organisations, businesses and individuals for their use of cloud computing services and that are normally aware of privacy requirements in different countries in the business context. On the other hand, however, there is a multitude of cloud computing services that are used by individuals. These cloud computing services are often free of charge and have been used for many years. Many of these business models are built on the further processing and usage of personal data for marketing and reselling purposes and thus can entail additional data privacy challenges in some cases.

The potential scale of cloud computing as well as its economic and social promise highlight the importance of further work to address these issues, many of which cannot be easily reconciled by even the most attentive cloud service providers. Some of the privacy implications of these services were or are being considered in other recent OECD work on the revised OECD (1980) *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (Privacy Guidelines) and current OECD (2013) work on “big data”, and the specific privacy implications of these services are therefore not discussed in detail in this report.

In addition, considerable cloud-related privacy work is underway by non-governmental stakeholders such as the Internet technical community and other standards organisations. These initiatives include consideration of how to address privacy within standards development and work on standards to support legal frameworks for privacy and data protection, covering aspects such as identity, trust, authorised access, data security and user preferences for the protection of personal data, both individually as well as in overarching privacy frameworks. Some examples of these initiatives are the OASIS Privacy Management Reference Model, the IETF Privacy Directorate.[11], the IAB Privacy Programme,[12] the IETF Privacy Extensions for IPv6 (RFC3041/RFC4941), the W3C Privacy,[13] HTML5 or Web Services activities, the Kantara Initiative P3WG,[14] the ITU-T Study Group 17, the ISO/IEC SC27 WG5 on ID Management and Privacy Technology and the ETSI Annual Security Workshop.

Current terms and conditions of cloud computing contracts

As described above, there is currently some uncertainty for cloud users regarding different legal issues. Many of these issues can and should be addressed by the contract a cloud user signs with a cloud computing provider. However, according to Bradshaw, et. al. (2010) who surveyed and analysed the terms and conditions (T&C) of standard cloud computing contracts offered by 27 cloud computing providers, at least to date, standard contracts often come with a lesser degree of certainty compared to traditional outsourcing contracts. According to the authors, many cloud computing providers "include elements in their T&C asserting wide-ranging disclaimers of liability or of any warranty that the service will operate as described, or indeed at all" (Bradshaw, et. al. (2010), p. 45). In addition, they observed that service level agreements (SLAs) are often formulated in terms as to exclude most of the service outage causes.

Remedies to these outages are often only provided in forms of credits against future services. Other issues, such as the threshold for disclosure to third parties, the preservation of data at the end of a contract or the legal system under which the contract is offered vary greatly from one provider to another. There may also be special issues associated with the provision of cloud services to consumers. In addition, the authors detected some patterns while analysing the different cloud service providers: Providers based in Europe or asserting the law of a European state for customers in Europe "will typically be less forceful in denying liability than those which are based in, and assert the legal governance of a US state" (Bradshaw, et. al. (2010), p. 45). Moreover, when the cloud business model relies on payments by the customer for a service, the cloud computing provider is likely to offer more in terms of remedies for outages and more often offers access to data after the termination of the contract. Overall, the authors acknowledge that T&C will evolve over time, but highlight that formulating T&C that are clear and concise, also in the area of privacy, continues to be a challenge.

Vendor lock-in and standard-based solutions

According to recent surveys among potential users of cloud computing, a lack of standards and a lack of widespread adoption of existing standards are seen as one of the biggest challenges. The lack of open standards is mainly a huge problem in the area of platform as a service (PaaS). In this service model, application programming interfaces (APIs) are generally proprietary. Applications developed for one platform can typically not easily be migrated to another cloud host. While data or infrastructure components that enable cloud computing (e.g., virtual machines) can currently be ported from selected providers to other providers, the process requires an interim step of manually moving the data, software, and components to a non-cloud platform *and/or* conversion from one proprietary format to another. As a consequence, once an organisation has chosen a PaaS cloud provider, it is, at least at the current stage, locked-in. Attempts have been made to extend general programming models with cloud capabilities (Schubert, et. al., 2010), however, these are still the exception. Consequently, some customers have the concern that it will be difficult to extract data from a certain cloud which might prevent some companies or government agencies to move to the cloud. Another concern linked to this is that users get very vulnerable to providers' price increases. Promoting open standards for APIs and further work on interoperability is the appropriate response to this problem.

Broadband infrastructure

The continued innovation of the Internet and Internet-based applications and business models including cloud computing continues to increase the amount of data that is transmitted via broadband communication infrastructures. The demand for bandwidth is thus expected to increase resulting in a possible challenge of data transfer bottlenecks from and to cloud computing providers, especially when data is transmitted across borders.

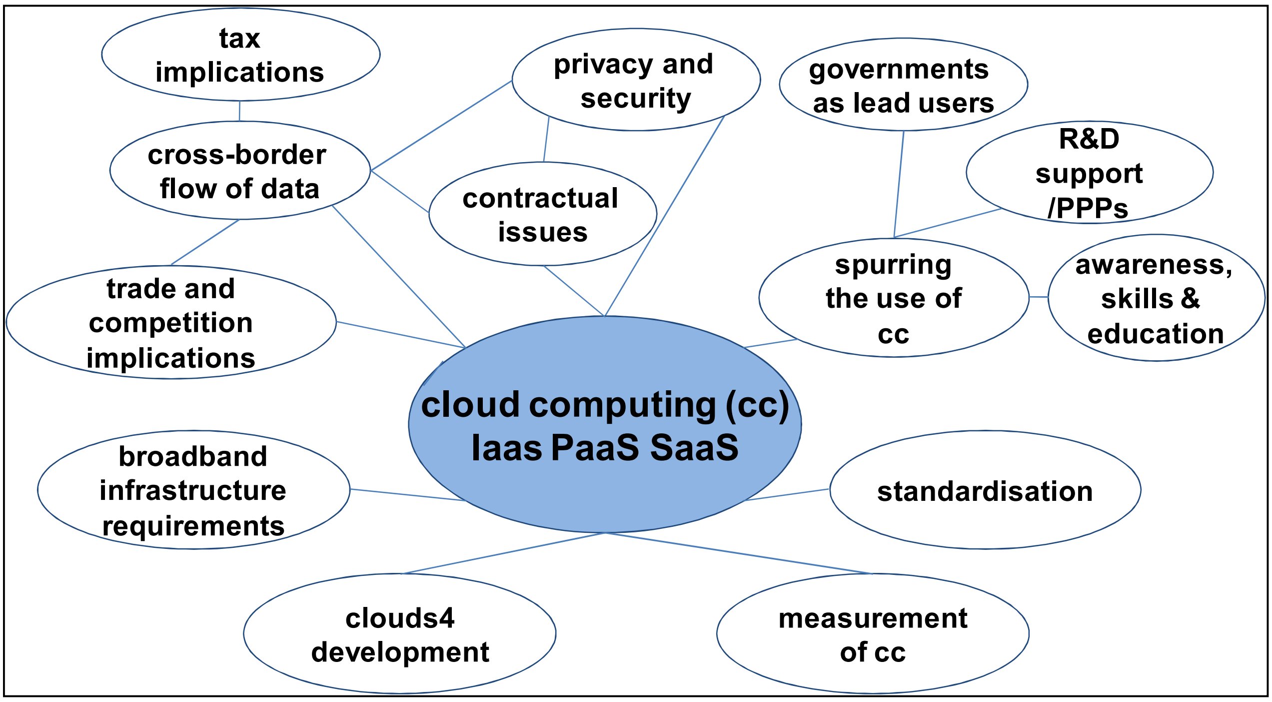
In addition, the importance of symmetric bandwidth increases with the further growth of cloud computing services as users move more of their data and applications to the cloud and want to process them online. Upload speeds thus will become a determinant factor for the use of cloud computing services. Currently, the download bandwidth is frequently 10-16 times higher than the bandwidth dedicated to uploads (OECD, 2009a) creating a dilemma for cloud computing users.

From a network-topology perspective, it is estimated that cloud computing does not significantly alter traffic flows significantly as the large cloud data centres typically have good fiber connectivity with Internet Exchange Points (see also Weller and Woodcock, 2013). The role of government and government policy

The role of government and government policy

This section of the report gives an overview of main policy areas in the area of cloud computing and the role of governments and international institutions. It discusses issues in more detail that are most relevant to the ICCP Committee and not dealt with by other OECD Committees. Figure 5 provides an overview of main cloud computing policy areas. It reveals that cloud computing has an impact on a multitude of very diverse areas.

Figure 5. Overview of main cloud computing policy areas



Spurring the use of cloud computing

As the section on the economic impact has shown, cloud computing can have beneficial effects on economic growth and especially on promoting the growth of small and medium enterprises (SMEs), including start-ups. Further, it may benefit consumers that already make important use of certain cloud applications such as e-mail services and online backup and synchronisation services. Overall, there are several ways of spurring the use of cloud computing, including, beyond removing unnecessary legal and regulatory barriers: i) raising awareness, developing skills and education, ii) governments as lead users of cloud computing; and iii) R&D support.

i) Spurring the use of cloud computing by raising awareness, developing skills and education

One major area of action is the contribution to a better understanding of the concept of cloud computing and its inherent benefits and challenges through openness and transparency. Since cloud services vary and since cloud computing has become a buzzword, there is a lack of a clear understanding of the concept. Though clouds have been identified as having many advantages for SMEs, SMEs in particular may have difficulties in fully understanding the concept. In addition, they may require additional support from the side of the cloud provider as they might not have the in-house expertise to effectively use cloud services.

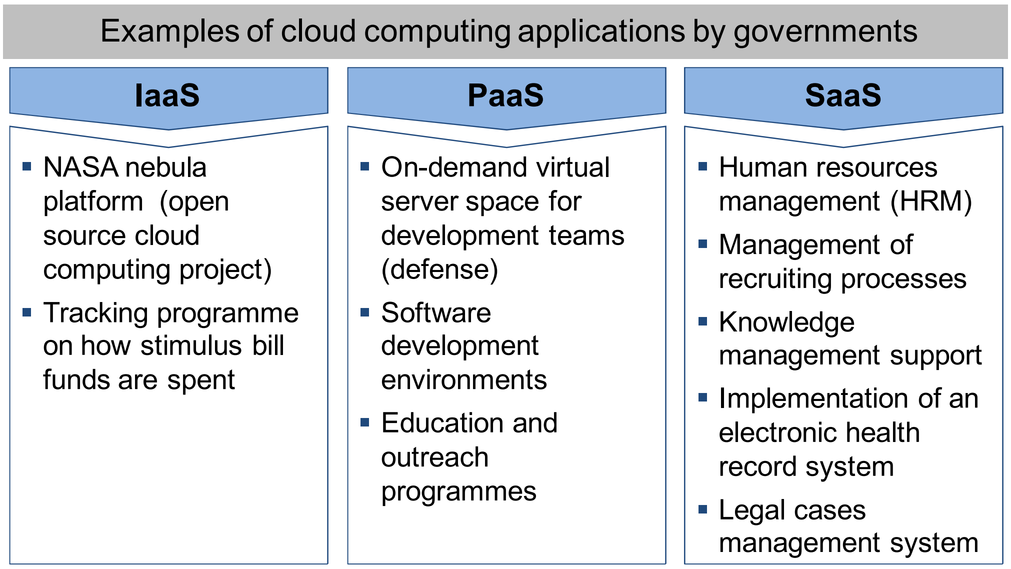
Governments could consider creating awareness in promoting and conducting educational activities (e.g. demonstrations of services, publications of studies on cloud computing) both at the business and consumer levels. Especially organisations that want to rely on cloud computing services instead of their own infrastructure have to acquire the necessary skills that allow them to do the right procurement choices and to be in a position to control and use these services. Some initiatives in this area are already under way: Germany, for example, has launched an overall action programme "cloud computing" that aims at encouraging the use of cloud computing in the German economy as a whole. In the area of skills, examples include programmes to improve the availability of skilled personnel such as Japan's ubiquitous town concept and Ireland's skill enhancement strategy.[15]

ii) Governments as lead users of cloud computing

Governments are important users of IT infrastructure. As cloud computing has the potential to significantly reduce costs and might increase energy efficiency, governments have launched several public cloud computing initiatives. The cloud service models in use range from cloud software as a service (SaaS) function (e.g. e-mail services, budget administration applications) to cloud infrastructure as a service (IaaS) function (e.g. the NASA Nebula cloud system) with SaaS functions largely prevailing (Kundra, 2010). Figure 6 provides some examples of cloud computing applications used by governments.

In terms of the current state of deployment of cloud computing, the United States government (USG) has taken a lead role. The USG leverages on all different cloud service models (see also Table 2) and it is actively spurring the further deployment of cloud computing services: It instituted a "Cloud First policy" which mandates agencies to evaluate cloud computing service options prior to making any new investment in IT (Kundra, 2010).

Figure 6. Examples of cloud computing applications used by governments



Currently, the Public Governance Committee (PGC) of the OECD is also undertaking work on cloud computing from a government user perspective in the context of the area of work of "Enabling Agile Governments". In order to avoid the duplication of analysis and content, PGC will look at the overall public governance issues that affect the development of government clouds and will study concrete case studies to show how governments use cloud computing to foster public sectors' efficiency and with agility. The result of this analysis will be discussed in a report that is expected to be finalised by the end of 2012.

iii) R&D support

In addition, governments could consider providing incentives for business R&D through public funding or public-private partnerships. This would be especially beneficial for initiatives targeted at developing open standards and platforms (see below). In addition, they have a role to play in fostering university research in this area for more long-term basic research as well as in encouraging universities to put their different IT networks together into a cloud to benefit from the advantages of this form of highly networked computing.

Standardisation

One of the major challenges is the lack of appropriate standards and the potential for vendor lock-in due to the use of proprietary solutions. Governments could encourage and support the development of cloud computing interoperability standards and use of the resulting standards. Standards should be conceived in a modular and adaptable way to ensure that they can be adapted to future needs and leave room for future innovation.

Many new initiatives are currently underway, covering the full spectrum from infrastructure standards, such as virtualisation formats and open APIs for management, to standards for web applications and services, security, identity management, trust, privacy and linked data. Initiatives include the following: The Swedish standardisation committee, "DIPAT" – TK 542 run by the Swedish Standardization Institute (SIS), launched an initiative to work on national and European level standardisation issues linking and aligning the initiative with global efforts run by Subcommittee 38 of the Joint Technical Committee 1 of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC 1/SC 38). The goal is to assist in the development of harmonised, sustainable and well designed standards. The final report of the ITU-T Focus Group on Cloud Computing is being used for starting new work within ITU-T. The European Commission is partnering with ETSI for cloud standards development. The IEEE has initiated two cloud computing specific projects (P2301 - Guide for Cloud Portability and Interoperability Profiles (CPIP) and P2302 - Standard for Intercloud Interoperability and Federation (SIIF)). OASIS has formed an Identity in the Cloud Technical Committee. Cloud computing standards that are being developed by the Distributed Management Task Force (DMTF) are being tracked into ISO/IEC with placement into JTC 1/SC 38. Additional standards organisations that currently also work on the issue include W3C, IETF, ETSI, OGF and the Kantara initiative. Finally, one of the top priorities of the European Commission - in the context of unleashing the potential of cloud computing in Europe - is to co-ordinate with stakeholders to identify a map of necessary standards by 2013 and to implement existing standards (European Commission, 2012).

Measurement of cloud computing

To this date, there are very few studies that try to measure cloud computing. This is partly due to the fact that the concept is rather new and that different definitions exist. Another reason is that policy makers currently do not have access to market data and that most companies do not report on their cloud computing revenues. As a future avenue, policy makers may begin initiatives to collect data on cloud computing. The data collection and the measurement should take both the supply and demand side into account. In addition, it could be interesting to monitor the cross-border flow of data as well as the location of the data.

Cloud computing for development

Due to the benefits mentioned above, cloud computing provides a very interesting means for organisations and consumers in developing countries. They can benefit from a various set of different computing resources that would otherwise not be available in many developing countries. As a consequence, cloud computing can provide a platform for the development of new businesses in these countries and improve societal development, including education, health care, and open government. Cloud services that are designed specifically for mobile phones and other mobile devices seem to be very promising as the deployment of mobile networks is often much more advanced than the deployment of fixed networks in developing countries.

However, there are also some challenges regarding the deployment of cloud computing in developing countries. First of all, many developing countries face challenges in the provision of electricity. Second, Internet infrastructure (i.e., wired or wireless broadband) needs to be in place providing a low-latency and robust Internet connection to cloud users. In addition, the majority of cloud computing providers are located in the northern hemisphere which means that an important percentage of overall Internet traffic has to go from the south to the north and back which can be expensive. A way to overcome this would consist in building up cloud computing infrastructure in developing countries. However, upfront investments to do so are high. Finally, there is a need to raise awareness of the benefits of cloud computing services, but also of the challenges and open issues.

Broadband infrastructure

With the growth of cloud computing services, the demand for bandwidth is expected to increase significantly and innovation in this field might also be driven by the availability of extensive bandwidth. Policy makers should thus promote the most flexible network technologies and topologies and spur competition so that future solutions that promote the most bandwidths can develop (OECD, 2009a). In addition, policy makers along with network planners should pay particular attention to the development of a network that can be easily adapted and supports capacity upgrades to higher future bandwidth demand.

Trade and competition implications

It is probably too early to evaluate the trade and competition implications of cloud computing. However, policy makers should keep in mind the possibility that anti-competitive practices could result from the domination by few companies. They should also keep in mind the relationship between the efficient flow of data across jurisdictions and the growth of cloud computing.

Tax implications

An area where work has probably to be carried out is the area of tax implications. There are both some potential benefits and challenges arising from cloud computing in the area of taxation. In terms of benefits, cloud computing could improve standards of record keeping, especially for SMEs. However, there are also some challenges, for instance, in the area of record keeping requirements for business purposes. Tax evasion attempts could be another potential challenge.

Contractual issues

As the section on cloud computing contracts has shown, there are still some challenges regarding standard cloud computing contracts. This is especially an issue for smaller companies and consumers that are not able to negotiate the cloud computing contract. Policy makers could urge cloud computing providers to do more in the area of privacy and security. In addition, service level agreements should address service outages more and concrete remedies to these outages.

Security and privacy

The section on security and risk management highlights that, since cloud computing is the pinnacle of networked computing, a thorough and holistic risk management becomes crucial in order to assure the availability, integrity and confidentiality of data. The OECD 2002 Security Guidelines provide an essential high level framework for addressing security in an opened and networked environment, *a fortiori* in the cloud. Key principles include risk assessment, security design and implementation, risk management and reassessment.

Regarding risk assessment, there is a challenge as users currently need to audit the security and privacy safeguards of a cloud provider. For large companies or big public agencies, an appropriate level of review is feasible and also currently undertaken. However, SMEs, start-ups and consumers might neither have the resources nor the skills to perform detailed assessments. Governments could thus encourage and spur the current development of sound security and privacy certificates of cloud services as well as certification programmes for IT professionals working in the area of cloud computing. In terms of security design and implementation, it is key to incorporate security as an important element in the network and IT infrastructure and to design and adopt the appropriate safeguards. In terms of security management, if the user decides to transfer the risk, it is crucial to carefully evaluate the terms and conditions of the contract with the cloud provider. Finally due to changing threats and vulnerabilities, it is important to continually review all aspects of security and undertake modifications in the security policy if needed.

In the area of privacy, many of the challenges noted above require additional work in appropriate international-level fora. The communiqué from the OECD's High-Level Meeting on the Internet Economy in June 2011 highlights the need to minimise barriers to the location, access and use of cross-border data facilities and function, through the implementation of appropriate data protection and privacy measures. It further calls for work to promote and protect the global free flow of information through increased global compatibility across a diverse set of laws and regulations, while also respecting fundamental rights. Progress in meeting these objectives would certainly benefit maturation of cloud computing.

Conclusion

Due to its potential impact on economic growth but also in light of the challenges raised by cloud computing, the analysis presented in this report suggest to continue work in this area. In particular, further trends in this area could be analysed. These could include the assessment of ways forward in the area of privacy and security and the impact of cloud computing: i) on fixed and wireless network infrastructures, ii) on the ICT sector (e.g. reshape of the sector, impact on the hard disk market, new cloud business models); iii) on IT departments of organisations and iv) public sector service delivery concepts. Other issues for further study could include: an analysis of i) cloud computing contracts; ii) data portability; iii) free flow of information principles. Finally, in the context of STI's horizontal work on innovation for development and the renewed emphasis on development at the meeting of the Council at Ministerial Level (MCM, 2011), work on cloud computing for development could be undertaken.

NOTES

1 Intellectual property rights (IPR) might also play a role in cloud computing to the extent that goods and services subject to copyright and trademark protection are delivered, disseminated and otherwise made accessible in the cloud. IPR issues, however, are not addressed in this paper.

2 The study covered the EU 27.

3 The aggregated sectors are: Manufacturing, wholesale and retail trade, hotels and restaurants, transport storage and communication, real estate renting and business activities.

4 The concrete number of jobs, however, is hard to measure owing to the heterogeneity of cloud computing providers, to the lack of data on their cloud computing activities, and to the multitude of services (OECD, 2010a, Chapter 3).

5 Rebound effects refer to the phenomenon that higher efficiencies at the micro level do not necessarily translate into equivalent savings at the macro level (e.g. economy-wide) (see Mickoleit, 2010). An increase in efficiency leads to lower costs which in turn may lead to more investments in new servers.

6 A measure often used in quantifying emissions is the measure carbon dioxide-equivalent (CO_2e) emissions. Different emissions vary in their warming influence, the radiative forcing, on the climate. The common metric which is used in many studies is the radiative forcing of CO_2. "The equivalent CO_2 emission is obtained by multiplying the emission of a GHG by its Global Warming Potential (GWP) for the given time horizon." (IPCC 2007).

7 Countries include: The Czech Republic, France, Germany, Poland, Portugal, Sweden and the United Kingdom.

8 Based on the diffusion theory that suggests that about 16-20% of the market will always resist adoption.

9 The authors define small organisations as organisations that have between 1 and 49 employees and on average 25.

10 www.informationweek.com/cloud-computing/infrastructure/amazon-web-services-hit-by-power-outage/240002170; www.huffingtonpost.com/2012/07/02/amazon-power-outage-cloud-computing_n_1642700.html.

11 www.ietf.org/mail-archive/web/ietf-announce/current/msg08294.html.

12 www.iab.org/activities/programs/privacy-program.

13 www.w3.org/Privacy.

14 http://kantarainitiative.org/confluence/display/p3wg/Home.

15 Source: Policy questionnaire of the OECD Technology Outlook 2010.

ANNEX

A.1 Vulnerabilities in the cloud

Areas where vulnerabilities are potentially reduced

To begin with, as a rule of scale, security measures are getting cheaper when adopted at larger scales. In addition, big cloud computing providers are able to create redundancy since many of them typically replicate data and applications in multiple locations making them more robust in the face of disasters. Due to their size, they are also in the position to hire specialists for very specific security threats and to dispose of an improved response timeline, for example, through the detection and the monitoring of new security threats (ENISA, 2009).

Second, even though the concentration of resources poses risks (see below), it has also some benefits regarding security measures on physical sites such as cheaper physical access control, cheaper application of a comprehensive security policy and maintenance processes (ENISA, 2009).

A third advantage of big cloud computing providers is their inherent capability to dynamically upscale computing resources dedicated to security measures, also and especially in the event of concrete security threats and attacks.

A fourth benefit consists in more timely updates and defaults. On a homogenous cloud platform, updates can be performed more rapidly than in traditional systems. In addition, applications and software can be pre-hardened, i.e. secured, with the most recent security settings and processes (ENISA 2009).

Finally, many surveys have shown that high levels of security and privacy are a crucial decision criterion for users and potential new users of cloud computing services (e.g., WEF 2010). The provision of a high level of security is thus a fundamental requirement for cloud computing providers and particularly high security levels constitute a significant competitive advantage. Cloud computing providers have thus an incentive to guarantee high levels of security and privacy.

Areas where vulnerability are potentially increased

Besides these benefits, cloud computing also presents vulnerabilities that are already known to most networked IT systems and affect the availability, integrity and confidentiality of the data stored in the cloud. Most of them result from the high level of networked computing inherent in cloud computing. The following paragraphs provide some illustrative examples.

A first challenge is a *loss of IT control and governance*. In terms of security, this could mean that conflicts arise between the security measures and procedures on the customer side and the cloud computing environment (ENISA, 2009) and that rules and responsibilities are unclear. As a consequence, this could lead to the impossibility of a cloud computing user to comply with its own security standards and could provoke compliance challenges, especially, if applications are run and data is processed and stored in multiple jurisdictions.

Another challenging characteristic of cloud computing is the fact that *customer management interfaces* of a cloud computing provider are usually accessed through the Internet. Those interfaces also mediate access to a larger set of resources and multiple tasks such as management, provisioning and monitoring. Consequently, they pose a security challenge, especially in combination with web browser vulnerabilities. This can be mitigated to a certain extent by more investments in the security of customer management interfaces and more specifically by ensuring strong authentication, access control as well as encrypted transmission (ENISA, 2009, Cloud Security Alliance, 2010).

A third *security challenge results from the resource pooling in public clouds and multitenancy* which means that different cloud users share the same physical infrastructure. Multitenancy becomes a problem when security mechanisms that separate memory, storage and routing between multiple tenants fail. How these mechanisms can fail is shown in Box A.1.

Box A.1 Multitenancy and security mechanism failure

The fact that cloud computing in public clouds relies on resource pooling and multitenancy can pose a security challenge. Multitenancy becomes a problem when security mechanisms that separate memory, storage and routing between multiple tenants fail. How these mechanisms can fail is shown in a study by Rispenpart et al. (2009). The authors show in a case study how to map the internal cloud infrastructure of a cloud computing provider, how to identify where a particular target virtual machine is likely to be located and how to instantiate new virtual machines until one is placed as a co-resident of the target. Finally, they illustrate how this placement could be used to launch attacks to extract information from a target. It has to be noted that the specific placement algorithms of the cloud provider considered in this study, Amazon EC2, allowed attackers to use fairly simple strategies. Overall, regarding the challenge of multitenancy, two aspects should be considered: First, there are several measures to mitigate this risk: The authors propose obfuscating the internal service structure and the placement policies in order to at least complicate attackers' attempts to place a virtual machine on the physical machine where the target is located (Rispenpart et al. 2009). For example, providers could impede network co-residence checks. Another way to mitigate this security challenge consists in concentrating on the side-channel vulnerabilities in order to prevent data leakage. Finally, the safest solution would consist in the fact that the cloud user would insist on an exclusive use of the physical machine. However, this would create opportunity cost as machines could potentially be underutilized. The second aspect to be considered is the actual risk of attack. These potential attacks should be evaluated against the risk of attacks on traditional solutions. According to ENISA (2009), attacks on isolation mechanisms have been less numerous and more difficult to perform than attacks on traditional operating systems.

Malicious insiders constitute a further example of a security challenge. As data of multiple tenants is stored on the same site, the impact of malicious insiders is typically more severe for cloud computing services than for traditional services. This is especially true for certain job roles such as system administrators and managed security providers. With the increased importance of cloud computing, these types of employees possibly become more and more popular targets for criminal activities. (ENISA, 2009).

Data protection is a further main security challenge that has been highlighted in many studies. These challenges can be categorised into technical and legal challenges, whereby the technical challenges are discussed in this section. From this perspective, besides the above mentioned vulnerability due to multitenancy, the *interception of data in transit* constitutes a challenge for data protection. In general, cloud computing involves more data transfer compared to traditional approaches. For example, data from cloud customers might be stored on several virtual machines in different locations which also includes the storage of several copies of data for redundancy purposes. Different attacks such as man-in-the-middle attacks or sniffing pose challenges for data protection. Another technical risk for data protection can arise while up- and downloading data to the cloud as *data leakage* can occur. Finally, as data is often stored in multiple locations, there is a risk of an ineffective, incomplete and insecure data deletion. When a cloud customer asks a cloud provider to delete data, data might still be available beyond the lifetime that was agreed. In addition, it might be very hard for the customer of cloud computing services to control whether data has been truly wiped. To lower this risk, encryption of data should be envisaged (ENISA, 2009).

A final challenge related to security includes the *availability of service*. For example, any situation where connectivity is degraded will prevent the delivery of the service, whether as a consequence of unintentional (e.g. a fiber being broken by accident or a power outage) or intentional failures (e.g. denial of service attacks). Recently, for example, some cloud computing services have been hit by power outages Another potential breach of availability may also result from business discontinuity of the cloud provider. Mergers and acquisitions could pose further challenges.

REFERENCES

Armbrust, M., A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia (2009), *Above the Clouds: A Berkeley View of Cloud Computing*, UC Berkeley Reliable Adaptive Distributed (RAD) Systems Laboratory, Berkeley, www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

Bradshaw, S., Ch. Millard and I. Walden (2010), "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*", Legal Studies Research Paper No. 63/2010, Queen Mary University of London*, School of Law, London.

Cloud Security Alliance (2010), "Top Threats to Cloud Computing v1.0", https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

ENISA (European Network and Information Security Agency), (2009), *Cloud Computing – Benefits, Risks and Recommendation for Information Security*, ENISA, Heraklion.

Etro, F. (2009), "The Economic Impact of Cloud Computing on Business Creation, Employment and Output in the E.U.", *Review of Business and Economics*, 54 (2), 179-208.

Etro, F. (2010) "The Economic Consequences of the Diffusion of Cloud Computing", in S. Dutta and I. Mia (eds.), The Global Information Technology Report 2009-2010, World Economic Forum, Geneva.

European Commission (2012), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Unleashing the Potential of Cloud Computing in Europe, COM(2012) 529 final.

Intergovernmental Panel on Climate change (IPCC), (2007), Climate Change 2007: Synthesis Report, Valencia.

Kundra, V. (2010), *State of Public Sector Cloud Computing*, US Chief Information Officers Council, www.cio.gov/documents/StateOfCloudComputingReport-FINALv3_508.pdf.

Kushida, K.E, J. Murray and and J. Zysman (2011), "Diffusing the Fog: Cloud Computing and Implications for Public Policy", BRIE Working Paper 197.

Mickoleit, A. (2010), "Greener and Smarter: ICTs, the Environment and Climate Change", *OECD Green Growth Papers*, No. 2010/01, OECD Publishing.
doi: 10.1787/5k9h3635kdbt-en

NIST (US National Institute of Standards and Technology, (2011) *The NIST Definition of Cloud Computing*, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

OECD (2013), "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", *OECD Digital Economy Papers*, No. 222, OECD Publishing. doi: 10.1787/5k47zw3fcp43-en

OECD (2010a), "ICT Skills and Employment", in OECD, *OECD Information Technology Outlook 2010*, OECD Publishing. doi: 10.1787/it_outlook-2010-5-en

OECD (2010b), ICCP Technology Foresight Forum - Cloud Computing: The Next Computing Paradigm?, OECD conference, 14 October, www.oecd.org/sti/ict/cloudcomputing.

OECD (2009a), *Network Developments In Support Of Innovation And User Needs,* OECD, Paris.

OECD (2009b), "Briefing Paper for the ICCP Technology Foresight Forum – Cloud Computing and Public Policy", *ICCP Technology Foresight Forum - Cloud Computing: The Next Computing Paradigm?*, OECD, Paris.

OECD (2002), *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD Publishing. doi: 10.1787/9789264059177-en-fr

OECD (1980), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris.

Perry, G. (2008), *How Cloud Computing and Utility Computing are Different*, http://gigaom.com/2008/02/28/how-cloud-utility-computing-are-different/.

Schubert, L., Jefferey, K. and B. Neidecker-Lutz (2010), *The Future of Cloud Computing: Opportunities for European Cloud Computing beyond 2010, Public Version 1.0*, http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf.

Thomond, P., Gann, D., MacKenzie, I. and A. Velkov (2011), *The Enabling Technologies of a Low Carbon Economy: From Information Technology to Enabling Technology: Can Cloud Computing Enable Carbon Abatement?, Summary Report,* www.enablingtechnology.eu/environment/academic_study .

Weichert, T. (2011), "Cloud Computing and Data Privacy", Working Paper, The Sedona Conference, Phoenix, AZ.

Weller, D. and B. Woodcock (2013), "Internet Traffic Exchange: Market Developments and Policy Challenges", *OECD Digital Economy Papers*, No. 207, OECD Publishing. doi: 10.1787/5k918gpt130q-en.

West, D. (2010), *Saving Money Through Cloud Computing*, Governance Studies, The Brookings Institutions, Washington DC.

World Economic Forum and Accenture (2010), *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation*, World Economic Forum, Geneva.

Wyld (2010), *Moving to the Cloud: An Introduction to Cloud Computing in Government*, http://www.etransform.org/gti/sites/etransform.org/files/Documents/2010-07%20IBM%20Business%20of%20Gov%20-%20Cloud%20Computing%20in%20Government.pdf.

Zittrain, J. (2009), “Lost in the Cloud”, *The New York Times*, New York, 20 July.