CLOUD ACCOUNTABILITY PROJECT

D:A-2.1 Project Horizons Report

Deliverable Number: D12.1

Work Package: WP 12

Version: Final

Deliverable Lead Org: HP

Dissemination Level: PU

Contractual Date of Delivery (release): 31st July, 2013

Date of Delivery: 31st July, 2013

Editors
Nick Wainwright, Nick Papanikolaou (HP), Vasilis Tountopoulos (ATC), Anderson Santana de Oliveira (SAP), Martin Gilje Jaatun (SINTEF), Simone Fischer-Hübner (KAU), Tobias Pulls (KAU), Giles Hogben (CSA), Daniele Catteddu (CSA), Melek Önen (Eurecom)

Contributors
Giles Hogben (CSA), Jean-Claude Royer (EMN)

Executive Summary

This is A4Cloud's Project Horizons report for month 10 of the project (July 2013). A4Cloud is a European Framework Programme 7 research project developing principles, models and tools for achieving accountability in the cloud. This report records the outcome of monitoring relevant developments in the state of the art, and classifies these by type – developments related to the market, developments related to end users and how they interact with the cloud and cloud service providers, developments in regulatory initiatives and standards, and technical advances. Some of the key findings of the report are outlined next.

First, we have identified reference architectures for cloud and noted that more work is needed in this space, particularly from A4Cloud's perspective, Reference architectures for cloud computing services have been actively developed, including proposals for private cloud reference models (e.g. by Microsoft) and security threat models. Still there is much opportunity to develop and extend these with security and privacy features.

We have surveyed standardisation activities extensively and noticed significant developments in Interoperability between cloud service providers, and organisations involved in such activities include CSA, CSCC, DMTF, ETSI, GICTF, ISO/IEC JTC 1, ITU, NIST, OGF, OMG, OCC, OASIS, SNIA, The Open Group, ARTS, and the TM Forum. Standards need to be actively monitored in A4Cloud, and from the interoperability point of view, data formats and interface specifications are especially important.

Ongoing work on improving trust between service providers is through certification, and A4Cloud should monitor closely the relevant activities of the EU projects CUMULUS and CIRRUS in this regard.

The Cloud Security Alliance is actively developing models and frameworks that are of direct relevance to A4Cloud, including the CSA Open Certification Framework (OCF), which is now operational, the new version of the CSA Cloud Trust Protocol, and the newly published CSA Privacy Level Agreement (PLA) framework. A4Cloud will develop tools and mechanisms that should comply with and/or be compatible with these frameworks.

The European Commission's NIS Public-Private Platform has only just been established (as of 17 June 2013), and within its remit are included the development of cybersecurity guidance and operational measures for cloud computing service providers and organizations that use such services. A4Cloud needs to participate in the Platform's activities and ensure accountability measures and metrics are taken into consideration in future proposed guidelines.

Of huge importance for A4Cloud's legal work packages is the revision of the European Data Protection Directive, which will impact every organization in the EU which stores, processes or otherwise handles personal data; accountability has been conceived as a key element of the new regulation, but until the latest proposal is ratified (the General Data Protection Regulation, the first draft of which was issued in January 2012), A4Cloud needs to monitor the European Union's activities and discussions on the matter. Many amendments have been proposed to the regulation, and when consensus is reached, this will need to be reflected in A4Cloud's concept and interpretation of accountability.

Advances in computing power, and research developments in security, need to be actively monitored. Homomorphic encryption could have a profound impact on the way data is stored and processed in the cloud, although efficient means of implementing it have yet to be found and may be unlikely during the lifespan of A4Cloud. Of more operational importance are the developments in format preserving encryption – notably, there is an increasing number of companies offering FPE based encryption services allowing clients of public cloud services to encrypt data stored and processed on these services, while experiencing minimal limitations in functionality. One example of such a product is Ciphercloud (see http://www.ciphercloud.com).

More broadly, there is growing activity on the political front, with end user movements on the rise and mounting pressure for open data from governments. A4Cloud is well placed to provide solutions that meet end users' needs as well as organizational requirements for accountable cloud computing ser-

vices. The recent revelations about the US government's PRISM programme, which allows government agencies to access foreign nationals' data outside US boundaries, have brought to the fore concerns about end user security and privacy which are directly relevant to A4Cloud, even though the frameworks and tools being developed within the project are not designed to counter government-scale surveillance.

Our findings seem to support the view that A4Cloud's objectives and proposed means of achieving those objectives are still very valid, relevant, and timely. As a project we will need to remain abreast of developments in standardisation and the proposed European Data Protection Regulation, since these two areas are developing most rapidly among the many areas surveyed during the preparation of this report.

Table of Contents

1 Introduction

The purpose of the WP:A-2 Project Horizons is to ensure that the activities and results of the project remain relevant despite the evolution and changes in the context surrounding the project that will undoubtedly occur during the lifetime of the project.

The name “Project Horizons” reflects the need to look as far as possible into the future to identify potential changes that will impact project activities as early as possible. In this context, ‘lifetime of the project’ stretches from the point the project was initially conceived in HP Labs in the summer of 2011 through to the end of the project in March 2016, a period of nearly five years. For example, we know that data protection regulation in Europe will be changing during the lifetime of the project (even though it may not be finalised and put into force before the A4Cloud project finishes) and, while we have a good idea of their broad directions, we do not know the specifics of the regulations that will emerge. Other changes are happening at the same time, new standards for security, assurance, and certification are emerging, social norms around privacy and the use of the internet are evolving, new initiatives from public sector, vendors, and users will likely emerge, and there is always the chance that some shock to the system – a security breach or breakdown in the market for cloud – could cause a radical change to the operating environment for the project.

This report is the first Project Horizons report and covers the period from summer 2011 (project idea) to summer 2013 (first half of 2013).

2 Methodology

The Project Horizons work package gathers inputs from a range of sources, analyses the data gathered, and provides insight to the Executive Board on the potential impact of the evolution of the context in which the project operates that might impact either:

- The activities and work of the project, or
- The potential for impact after the lifetime of the project.

The A4Cloud Project Stakeholder Map (see Figure 1, taken from deliverable D:B-3.1 Appendix A) identifies the stakeholder groups that are involved in the provision, use and governance of data in the cloud. This is based on the NIST taxonomy of cloud computing entities* which has been extended with key stakeholders for A4Cloud. This provides a “big picture” view of the areas where external changes

* See http://www.cloudcredential.org/images/pdf_files/nist%20reference%20architecture.pdf

and evolution may occur. For the purpose of exploring Project Horizons we have divided the external context into five broad areas which are based on the A4Cloud stakeholder map (Table 1).

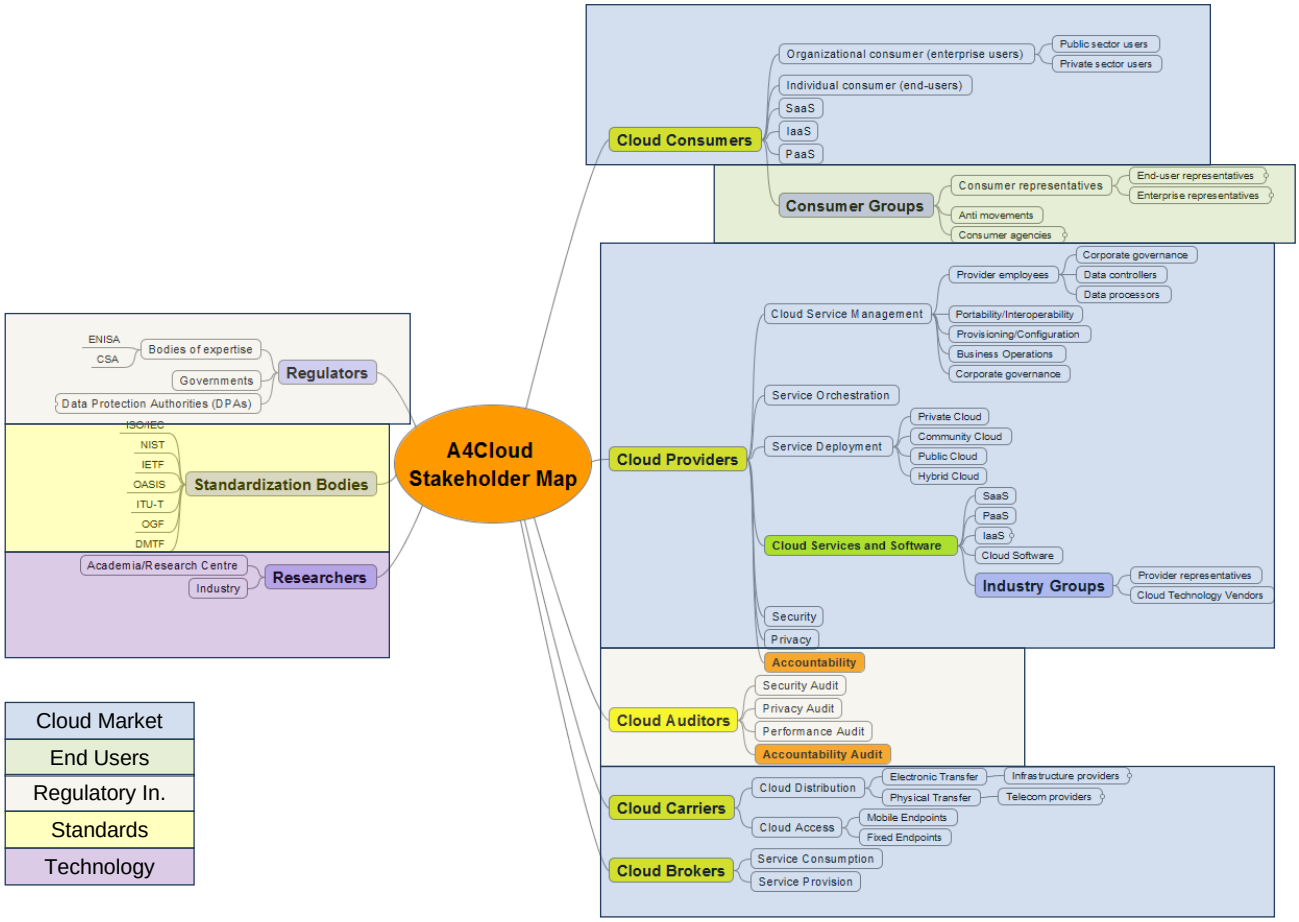

Figure 1 A4Cloud Stakeholder Map

The five groupings that we have used to explore the context are shown in the table below.

Area	*Description*	*Partner Responsible*
The Cloud Services Market	Broadly the cloud service providers and their customers in the private and public sector comprising the providers and business users cloud services	ATC
End-Users	Broadly this represents the individual users of cloud services through their personal and mobile devices using services and apps	SINTEF
Regulatory Initiatives	In particular data protection initiatives but also including the commercial legal frameworks for officering cloud services	HP
Standards For Cloud Services	Standards covering all relevant aspects but in particular those related to security, interoperability, certification, gov-ernance, etc.	CSA
Technology Shifts	Significant technology shifts that lead to new products and services for example the impact of big data and analytics, new cloud platforms capabilities, etc.	SAP

Table 1 Areas for Analysis

The partners in the project are well connected through a network of multidisciplinary contacts in industry, technical, regulatory and socio-economic actors in cloud and cloud governance. The source of information is therefore the partners in the consortium and their networks along with the projects advisory board.

A number of methods for gathering input are being used including brainstorm/collaboration sessions at project general meetings, polling individual work packages and partners for inputs, reports from attendees at major events and conferences, as well as monitoring the trends in the relevant areas, as they are depicted in the market analysis document on the Internet.

A key activity of the project horizons work package is analysing the inputs received from Stream leaders and the materials generated at brainstorming sessions. The purpose of the analysis is to rank risks and exploitation opportunities so that they may be acted upon by Stream and WP leaders. For risks/opportunities that span across several work packages, we will devise an action plan/strategy that will serve as an appropriate response – e.g. changing the focus of certain deliverables, bringing forward deliverables to ensure their timeliness.

Formal reports are produced in M10 (this report) and M42 which will be a summary of the information and analysis received.

3 Review of the State of the Art

In this section we review significant developments in the state of the art; in line with the principal research areas that cut across the A4Cloud project, we divide the review into seven subtopics: trustworthy architecture and protocols for interoperability, privacy assurance, trust assurance, management and governance frameworks, security and trust economics, security policies and related measures, and transparent security. For each topic, we have identified known limitations, which A4Cloud is indented to address, as well as the current status of each (esp. to what extent such limitations have been addressed, and what ongoing efforts exist to address them). In this section we consider specific developments that are related to the topic groupings in the A4Cloud Project's formal Description of Work. In Section 4 we will discuss developments more broadly, without reference to those particular groupings.

3.1 Trustworthy Architecture and Protocols for Interoperability

Current limitations (as stated in A4Cloud DOW)	**Status**
Proliferation of standards. *Inability to uphold specific regulatory requirements, users' choices and specific processing purposes.* *Reference architecture for accountability across the cloud.*	While the NIST Cloud Computing Reference Architecture† (NIST SP 500-292) includes security and privacy as two core elements in a cloud service provider's overall system architecture, the details of these are not described. The NIST Security reference architecture is available‡ and relevant here. Widely accepted architectural components for providing security and privacy functionality have yet to be devised. The Carnegie Mellon Insider Threat Security Reference Architecture§ does mention architectural components that could be of relevance to A4Cloud, although certain access controls are not relevant to a cloud scenario (e.g. physical security is outside the project scope).

† See http://www.cloudcredential.org/images/pdf_files/nist%20reference%20architecture.pdf
‡ - See http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf
§ See http://www.sei.cmu.edu/reports/12tr007.pdf.

	Several reference architectures for cloud computing have been proposed in the literature, including for instance the recently updated Private Cloud Reference Model from Microsoft[**], which presents a reference architecture for private clouds, consisting of six layers: a service delivery layer, a software layer, a platform layer, an infrastructure layer, a service operations layer and a management layer. This architecture is relevant to A4Cloud as it describes functionalities built into services by cloud providers; it does not explicitly name privacy and security controls. The CSA TCI reference architecture[††] is directly relevant here, in addition to the previously mentioned NIST materials.
Interoperability with existing frameworks, products, standards and approaches.	The IEEE Standards Association has an ongoing project, P2302 – Standard for Intercloud Interoperability and Federation (SIIF), which also includes governance elements; in case the standard is adopted widely in future, A4Cloud needs to be aware of the relevant data formats and mechanisms proposed by this working group. The Cloud Standards Wiki[‡‡] lists a large number of working groups and standardization activities that are likely to shape interoperability between different cloud service providers. Groups mentioned there include CSCC, DMTF, ETSI, GICTF, ISO/IEC JTC 1, ITU, NIST, OGF, OMG, OCC, OASIS, SNIA, The Open Group, ARTS, and the TM Forum. Standards need to be actively monitored in A4Cloud, and from the interoperability point of view data formats and interface specifications are especially important. The A4Cloud milestone document D:C-3.1 details all the standardisation activities we are aware of to date within A4Cloud.

3.2 Privacy Assurance

Current limitations (as stated in A4Cloud DOW)	**Status**
Lack of automation. Manual verification of adequacy of data handling controls is extremely costly. *Policy compliance checking and data tracking tools.*	Zawoad et al. [1] recently proposed SecLaaS, a tool for providing Secure Logging-as-a-Service for cloud forensics. SecLaaS provides confidentiality of logged data by public-key encryption, order preservation by cryptographic hashing, and integrity by the use of accumulators. Auditors have the ability to read *all* logged data, while users (of the logging service) only provide data to log. Write-once, read-many (WORM) devices (see e.g. [56]) are potentially relevant here. Sundareswaran [57] is also relevant here. In A4Cloud, one of our approaches is that users can read the data they log, and auditors are given access by man-

[**] See http://social.technet.microsoft.com/wiki/contents/articles/4399.private-cloud-reference-model.aspx
[††] See https://cloudsecurityalliance.org/research/tci
[‡‡] See http://cloud-standards.org/wiki/index.php?title=Main_Page

	date from users as required. We further protect the privacy of users' data by hiding the fact that some piece of encrypted data relates to a particular user. This goes beyond the "all or nothing" trust in auditors, only providing access to a particular set of logged data belonging to a particular user. Furthermore, we reduce the trust required in the logging service by preventing it from ever accessing the plaintext of the logged data. Interaction with the logging service is also auditable itself by another third party.

3.3 Architectures, Protocols and Models for Trust Assurance

Current limitations (as stated in A4Cloud DOW)	**Status**
Inherent complexity and context-dependence in notion of trust. *No consensus on evidence required to assess trust mechanisms. No suitable metrics exist for accountability.* *Support chain of accountability mechanisms.* *Support enhancement of external audit and produce an accountability tool providing evidence for external certification.*	Much work continues to be needed on metrics for trust in the cloud context. One approach to improving trust between service providers is through **certification**, and A4Cloud should monitor closely the relevant activities of the EU projects CUMULUS and CIRRUS. Standardisation activities currently in progress such as CSA's Open Certification Framework and ISO 27017 should also be monitored.

3.4 Management and Governance Frameworks

Current limitations (as stated in A4Cloud DOW)	**Status**
Existing frameworks are not specifically designed for dynamic data flows and rapidly changing technologies and business models. They are too generic to provide guidance on implementation of cloud-specific measures.	The Cloud Leadership Forum[§§] has a detailed model of the cloud governance lifecycle, dividing the whole process into five stages: (1) Cloud Strategy and Planning, (2) Cloud Architecture, Design and Deployment, (3) Cloud Acquisition and Contracting, (4) Resource Provisioning and Management, (5) Cloud Contingency Planning and Resource/Provider Management. This model mentions the development of a cloud security model in stage (2), and in A4Cloud this governance lifecycle should be taken into consideration and possibly adapted/extended. The SOCCI Framework Technical Standard[***] also presents a model for governance in the cloud which should be taken into consideration. CSA Open Certification Framework (OCF) is now operational and has successfully completed initial pilots for third party certification component. Auditor training will begin in October 2013. CSA Cloud Trust Protocol has issued a first draft of Model, API and metrics/properties documents and chartered a new working group which will begin work in September 2013. CSA Privacy Level Agreement (PLA) framework was recently published (February 2013).

[§§] See https://www.eiseverywhere.com/file_uploads/8d78b669e86b0120d704469d84fbf680_CLF_2011_Governance_Frameworks_Eric_Marks.pdf

[***] See http://www.opengroup.org/soa/source-book/socci/governance.htm

	ISO 27017 has not progressed further towards publication. It seems unlikely to reach final approval before 2015. ISO 27018 (data protection and privacy controls for cloud) is reaching final publication stage and is likely to become a stable public draft in early 2014. The European Commission has issued a call for Pre-commercial Procurement for Cloud, and the project has been selected and agreed. The ETSI CSC Task Force is currently producing a second draft of the list of security standards relevant to cloud. The list is planned for Q4 2013. The main areas of interest for standardisation identified by the ETSI task force so far are: Portability, Interoperability, Reversibility, and SLA. The Cloud Selected Industry Group is working on a list of suitable certification for cloud services, a code of conduct model and guidelines on SLAs. The SIG and ETSI CSC activities are meant to implement Action 1 of the European Cloud Strategy.

3.5 Socio-Economic Framework to Improve Security and Trust Economics

Current limitations (as stated in A4Cloud DOW)	**Status**
Liability assignment is difficult. *Current risk assessment methods are not tailored to cloud computing.* *Globally appropriate schema of risks and liabilities and best practice risk allocation.* *Models of risk and trust within the service provider ecosystem, including socioeconomic implications of risk.*	According to the Cloud Security Alliance's Top Threats to Cloud Computing[†††], these issues remain relevant; it is very difficult to assign responsibility and to decide whether to trust an entity with an unknown risk profile. The recently established (as of 17 June 2013) NIS Public-Private Platform of the European Commission aims to "bring together relevant European public and private stakeholders, to identify good cybersecurity practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions". Focus areas for the NIS Platform include organisational measures (practices to define, guide, and evaluate an organisation's cybersecurity risks), secure products and services (practices to demonstrate level of cybersecurity performance), metrics and measurement of cyber risk, and more. Clearly this initiative will be of great relevance to A4Cloud, and A4Cloud may be able to provide useful guidance on appropriate practices. The proposed EU cybersecurity directive and strategy[‡‡‡] is also directly relevant to the A4Cloud activities.

††† See https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

‡‡‡ See http://www.enisa.europa.eu/media/news-items/new-eu-cybersecurity-strategy-directive-announced

3.6 Interoperable Governance and Security Policies and Measures

Current limitations (as stated in A4Cloud DOW)	**Status**
Existing security languages are not able to handle accountability. *Competition law enforcement action risk.*	We have performed an extensive analysis of the current approaches for security models, languages, and standards in A4Cloud project milestone MS:C-4.2. There is a lack of explicit support to accountability concerns in the security frameworks for the cloud. Furthermore, CSA recently proposed to define privacy level agreements (PLA) to be used alongside cloud service agreements. The proposed PLA outline also covers some of accountability obligations such as data retention, personal data breach notification. The C4 work package aims at designing a new policy language by extending and/or combining existing languages and new enforcement mechanisms to fulfil accountability requirements. Also of interest is the ENDORSE[§§§] project's approach; this project has ended, but it is worth considering their way of linking legal data directives with policy enforcement.
No existing models for handling data governance and control within multi-tenant, complex and dynamic environments.	CSA is proposing the GRC stack [2] for governance, risk, and compliance on the cloud. Strategically, A4Cloud needs foster adherence to CSA's GRC stack not only to advance the state of the art, but also to increase the potential impact of the project's results. The approach taken by Wang and Zhou [58] may serve us well here.

3.7 Transparent security

Current limitations (as stated in A4Cloud DOW)	**Status**
Existing cloud transparency protocols are not privacy friendly. *Unfair terms of service by some cloud service providers.* *Current and future Data Processing infrastructure is far beyond user (and especially consumer) comprehension.* *Usability aspects of security are still an unsolved problem.*	The CloudTrust protocol has evolved from version 2.0 to version 3.0, aiming to offer a novel approach to compliance and accountability in the cloud – see above.

4 July 2013: Evolution, Changes, Developments of Relevance

This section provides a summary of relevant evolution and changes since the project was conceived in the summer of 2011.

[§§§] See www.ict-**endorse**.eu/

4.1 Cloud Services Market

4.1.1 Cloud Service Market Forecasts

Cloud-based solutions are being used in a wide range of business domains. Both public and private clouds are being established to satisfy the continuously increasing requirements of big data and its effective processing. Public clouds are leading to the emergence of new business paradigms and economic developments [3]. Worldwide spending on the cloud service market is expected to surpass $109 Billion in 2012 [4].

IDC [5] forecasts for 2020 cloud adoption are ambitious: they are expecting an increase of EU GDP up to €250 billion and the creation of more than 3.8 million jobs. However, such forecasts do not take into account the significant barriers to wider adoption of public clouds, namely the major concerns cloud service users. The same IDC study reveals great concern among different cloud stakeholders, concerns around the legal, technological and societal implications of cloud computing.
A recent IDC report [6] shows that EU enterprises maintain a good representation among cloud adopters, but most of them are far from driving sustainable and competitive business in the cloud proving that there is still a long to run towards real and beneficial cloud adoption, especially due to the immaturity of solutions to address the accountability needs of the cloud end users.

A4Cloud developments are well placed in this direction. Cloud models are inventing the ICT market as a new end-to-end IT service delivery paradigm, which is expected to grow rapidly [7]. Especially, the involvement of many players in the cloud service provisioning chain makes the A4Cloud support for preventive, detective and corrective mechanisms for accountability in the cloud an apparent immediate need, when managing, processing and storing personal and corporate data in remote spaces.

4.1.2 Cloud Provider Landscape

A number of enterprises have already started, offering solutions for managing data and processes in off-premise spaces [8, 9, 10, and 11]. The top of them seem to offer hybrid cloud solutions in different models (PaaS, SaaS and IaaS) [12] and are ranked as depicted in Figure 2, which has been taken from the August 2011 study in [13]. In this study, transparency and auditability are deemed as critical evaluation factors, and the results show that the existing vendors lack on convincing solutions for cloud security. A4Cloud can fill in this gap, irrespective on the fact that these vendors act simultaneously as both service and infrastructure providers.

The Cloud Market: Ranking the Solutions (4 = Highest Score)

Roll-Up Scores	VMW	MSFT	AMZN	IBM	HP	CA	RAX	BMC	RHT	ORCL
IaaS + Mgmt.	3.6	2.6	2.4	2.4	2.4	2.4	2.3	2.2	1.8	1.0
PaaS	3.7	3.1	2.4						2.2	1.7

Figure 2: Ranking the cloud vendors in providing IaaS, management and PaaS solutions in the cloud. The acronyms correspond to stock ticker symbols for VMWare, Microsoft, Amazon, IBM, HP, Computer Associates, Rackspace, BMC Software, RedHat and Oracle.

From a marketing perspective, an interesting analysis comes from Gartner [14], in which cloud IaaS providers are placed in the magic quadrant, as shown in Figure 3. This graph can offer insight into which are the representative IaaS providers that A4Cloud can approach in order to raise awareness in developing its accountability framework.

Figure 3: IaaS providers in the Gartner magic quadrant

Examining the evolution of the cloud provider landscape as depicted in [15], A4Cloud can gain from the predictions made there on the priorities of the cloud providers in the next five years. Such priorities can be taken into consideration so that the target engagement groups and tactics are adapted to the evolution of the cloud providers' trends and form the final group of stakeholders to be approached towards the end of the project.

4.1.3 Issues in Cloud and Security Fields for Cloud Providers

While bringing innovations to business transactions, clouds create a number of issues and problems especially in the field of security. The benefits from both public and private clouds have been successfully assessed by the European Commission and specific actions have been proposed in the September 2012 EC report, Unleashing the Potential of Cloud Computing in Europe [16]. These actions are around three dimensions:

- The support of trusted cloud services through well recognised and widely accepted standards. A4Cloud is well placed, since the project aims to follow NIST and collaborate with ETSI and ENISA as the identified standardisation bodies to lead this key action
- The uncertainty of the regulatory framework and the lack of legal terms to move away from the complexity of rules in contracts and SLAs. A4Cloud invests in the legal dimension and conducts research in the implications of the legal barriers to the cloud computing in order to support accountability.
- The European Cloud Partnership, which aims at successful leadership of European enterprises in cloud service provisioning.

In December 2012, ENISA published the report on CIIP perspective on cloud computing services [17]. This report follows the A4Cloud approach of supporting preventive mechanisms towards accountability in the cloud. Specifically, security governance should be based on appropriate risk analysis and assessment strategy, which entails the incorporation of key security measures to predict security incidents, the definition of proper mitigation strategies and the collection of incident reports as a corrective mechanism to update and assess the risk assessment strategy.

On the legal dimension of accountability, A4Cloud will be aligned to the latest evolution of the European Parliament directive with respect to cyber security [21]. Cloud providers need to conform to certain technical and organizational rules concerning the processing of personal data and the protection of privacy in all electronic communications

A4Cloud research and development will significantly support the cloud provider landscape in effectively drawing their security strategy for their cloud customers. As per PwC in [22], although cloud technologies are mature, the support for security is lingering with less than 40% of the enterprises drawing up security strategic plans. This is a barrier to cloud adoption, which A4Cloud can remove by supporting cloud providers in delivering mechanisms towards accountability in the cloud. To this end, A4Cloud develops a framework to leverage accountability in cloud providers and other stakeholders by building on top of existing security controls (as suggested by NIST in [23,24,25]) and extending them efficiently to deploy accountable cloud operations to provide high end services in the cloud.

4.2 End Users

In this context, the term end user is interpreted only as individual (private) consumers, not enterprise users. In the stakeholder taxonomy, however, we also cover consumer groups of different types.

A recent study by technical support firm FixYa [26] indicates that security remains the largest concern for users of cloud storage services Dropbox (40%) and Box (25%). Interestingly, tough, the same survey also queried users of cloud services Google Drive, Sugarsync, and iCloud, but none of these users seem to have mentioned security as a concern. From the very limited documentation provided, the reasons for this are not apparent, but we may speculate that it is related to lack of public security incidents as experienced by Dropbox [27] (and it is entirely possible that due to the similar name, Box is tarred with the same brush as Dropbox), and possibly because users don't stop to think about how a service like iCloud is realized, since it essentially is delivered as part of the iPad or similar operating system.

Internet users in Europe are worried about how the uncurbed powers of the Patriot Act allow US authorities free access to any data stored on US territory, even though industry analysts suggest data is not necessarily better protected in Europe [28]. In this case it may be, however, that end users are more comfortable with "the devil they know", and the "distance of redress" is certainly shorter to a national authority than to an agency across the Atlantic. Of course, even more worrying is the potential for US authorities to access data on EU territory.

The Electronic Frontier Foundation (EFF) argues that although the privacy issues involved actually predate cloud computing (and even the internet), cloud computing exacerbates the problem, since it enables European use of American infrastructure, also for individuals, on a scale that previously would have been infeasible [29]. Furthermore, EFF points out something which was raised at the first A4Cloud stakeholder workshop: that US authorities can demand disclosure of data hosted by US companies (e.g. Google or Amazon), even if this data is not stored physically in the US, but rather in data centres in, e.g., Ireland. At the A4Cloud workshop it was stated that this particular challenge was solved by European companies by establishing separate legal entities for their US operations; these entities would then have no "control" over data stored by the parent company in Europe. The recent revelations about the PRISM programme have however revealed that content is also accessed by authorities[****]...

Surveys show that people (end users) don't agree on whether governments should be able to 'go beyond the law' in this way or not; 51% of queried US people thought it was a good thing, while 38%

[****] See https://www.cerias.purdue.edu/site/blog/post/opticks_and_a_treatise_on_the_prism_surveillance_program_guest_blog/

thought it went too far††††. 42% said that the government should be able to go beyond the law, whereas 45% said that the law should always be adhered to. This clearly shows a divide among the US population. Nor has the PRISM disclosure gone unnoticed in other countries; non-US citizens are after all the main target of the PRISM programme. Australian privacy advocates demanded that their government disclose information on how much local data is reported to US security agencies‡‡‡‡. Sir Tim Berners-Lee described the NSA surveillance as an "intrusion on basic human rights"§§§§, and that internet users should be informed when another party stores or accesses data. They should also have a right to be informed when someone requests or stores their data*****. There are clear correlations between this reaction to public surveillance and the accountability of cloud services that is the main target in A4Cloud.

Apple co-founder Steve Wozniak has voiced his personal reservations about cloud computing in the past, and without using the term "accountability" has said that he sees a lack of transparency and that providers are unwilling to take responsibility for any events that happen in the cloud. Wozniak's proposed solution is more regulation, which might be a surprising statement from an American entrepreneur [30]. Various cloud provider representatives responded to this debate by proposing several surprisingly problematic solutions [31], such as encrypting data stored in the cloud (which doesn't solve availability concerns, and its effectiveness depends on who has access to the encryption keys and how they are managed), storing copies locally or at competing providers (doesn't solve confidentiality/privacy concerns, and introduces data synchronization challenges), or simply admitting defeat through stating that "perhaps […] sensitive data may not be ready to be put up into the cloud yet".

It has become typical for cloud service providers to use services from other providers. If one of the providers in the chain has problems, who is to blame for the issues? Network World describes how this situation makes it difficult for you to see how a company's partners use and store your data†††††. Examples also show how this model threatens data security. By hacking a third party application that had direct access to Yahoo's databases they could be infiltrated‡‡‡‡‡.

Relying on only the largest providers and putting all eggs in the same basket could also prove problematic. Richard Stallman in 2008 warned that cloud computing would result in vendor lock-in§§§§§. In 2013 we are now starting to see possible signs that companies are shifting tactics.

The organization EuropeVsFacebook [32] is targeting Facebook as a company they claim is not abiding by European privacy legislation. They do not focus on the fact that Facebook is a cloud service, but rather on the general problems faced when balancing privacy legislation against a business model which is based on making users share a lot of information with other users. The European Digital Rights organization, which coordinates the activities of around 35 European privacy and civil rights organizations, has also commented critically on the Irish DPA's seeming inaction in cases of privacy complaints against Facebook [33].

4.3 Regulatory initiatives

There are several organisations and initiatives which need to be monitored by A4Cloud as their potential impact on the outcomes of the project is significant. These can be grouped into three broad classes: (i) public sector initiatives, including national and pan-European initiatives; (ii) the European legislative bodies in charge of delivering the new Data Protection Directive and related laws & regulations,

†††† See http://www.huffingtonpost.co.uk/2013/06/10/poll-finds-public-support-snooping-plans_n_3415724.html

‡‡‡‡ See http://www.abc.net.au/news/2013-06-11/privacy-advocates-demand-internet-data-surveillance-transperancy/4746696

§§§§ See http://www.wired.co.uk/news/archive/2013-06/10/berners-lee-nsa-prism

***** See http://www.theinquirer.net/inquirer/news/2273826/web-inventor-tim-bernerslee-calls-on-internet-users-to-demand-legal-protection-from-prism

††††† See http://www.networkworld.com/newsletters/stor/2011/071811stor2.html

‡‡‡‡‡ See http://www.ibtimes.co.uk/articles/430062/20130131/cloud-computing-security-problems-being-ignored.htm

§§§§§ See http://www.guardian.co.uk/technology/2008/sep/29/cloud.computing.richard.stallman

and (iii) international (meaning specifically non-EU) initiatives. These are detailed in the following sub-sections.

4.3.1 Public Sector Initiatives

4.3.1.1 National Initiatives: UK GCloud – Government Cloud

The UK Government has adopted a strategy for the adoption of cloud computing across government services. In particular, a commodity marketplace of ready-to-use cloud services that are certified for government use was been established at http://gcloud.civilservice.gov.uk/ prior to the start of A4Cloud.

The metrics and certifications that are being adopted as part of the GCloud programme are essentially sets of requirements and expectations that cloud service providers must meet in order for their offerings to be acceptable for government use; from the point of view of A4Cloud, these requirements are likely to be useful in guiding the design of assurance capabilities, and metrics for accountability.

4.3.1.2 European Cyber Security Strategy

The European Cyber Security Strategy (ECSS for short) sets out the principles for cyber security that support the EU's core values, including (a) protecting fundamental human rights, freedom of expression, personal data and privacy, (b) access for all, (c) democratic and efficient multi-stakeholder governance.

The ECSS identifies the actions that will be carried out by the European Commission and ENISA to support the Commission's strategic priorities (namely: achieving cyber resilience, drastically reducing cybercrime, developing a common cyber defence policy, developing industrial and technological resources for cyber security, and establishing a coherent international cyber space policy for the EU).

Among the actions identified in this report, there are mentions of cyber incident exercises, the development of the recently established European Cybercrime Centre, and the stimulation of industry-led security standards.

All of these activities must be monitored and taken into account when implementing the accountability tools in A4Cloud, so that they support the standards and capabilities developed at the European level.

4.3.1.3 European Cloud Strategy

The European Cloud Strategy, discussed in [34] and expounded in [35], involves activities that are of significant relevance to A4Cloud. Among these, the development of model contract terms for cloud computing contracts is directly related to the D-4 Contracts and SLAs work.

The creation of a 'European Cloud Partnership' and associated funding of 10m Euros for a Pre-commercial procurement project to harness the public sector's buying power, which is planned to be completed in 2013, will likely impact the landscape of cloud service provision and the associated business models. For A4Cloud this could impact how accountability services are sold to the public sector.

4.3.1.4 ETSI

ETSI, the European Telecommunications Standards Institute, produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. ETSI is recognized as a standards organization, and in the context of cloud computing it is coordinating with stakeholders in order to build a map of standards required in the areas of security, interoperability, data portability and reversibility.

From the point of view of A4Cloud it is important to monitor the standards identified by ETSI and to ensure project results are suitably aligned. Of course, A4Cloud is uniquely placed to influence accountability standards for the cloud.

4.3.2 Data Protection Regulations (EU)

An extensive reform of EU data protection rules is underway, with significant implications for A4Cloud's analyses and results. Accountability is a key principle being adopted in the revised legislation, which is still far from complete and is currently being debated in the European Parliament. The revised legislation will hopefully be adopted by the end of Summer 2017. Some highlights of the changes under discussion are listed below – the text is quoted from [36].

- *"A **single set of rules** on data protection, valid across the EU. Unnecessary **administrative requirements,** such as notification requirements for companies, will be removed. This will save businesses around €2.3 billion a year.*
- *Instead of the current obligation of all companies to notify all data protection activities to data protection supervisors – a requirement that has led to unnecessary paperwork and costs businesses €130 million per year, the Regulation provides for increased **responsibility and accountability** for those processing personal data. For example, companies and organisations must notify the national supervisory authority of serious **data breaches** as soon as possible (if feasible within 24 hours). Organisations will only have to deal with a **single national data protection authority** in the EU country where they have their main establishment. Likewise, people can refer to the **data protection authority** in their country, even when their data is processed by a company based outside the EU.*
- *Wherever **consent** is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed.*
- *Citizens will have easier **access to their own data** and be able to **transfer personal data** from one service provider to another more easily (right to data portability). This will improve competition among services.*
- *A **'right to be forgotten'** will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it.*
- *EU rules must apply if personal data is **handled abroad** by companies that are active in the EU market and offer their services to EU citizens.*
- ***Independent national data protection authorities** will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules. This can lead to penalties of up to €1 million to 2% of the global annual turnover of a company.*
- *A new **Directive** will apply general data protection principles and rules for **police and judicial cooperation** in criminal matters. The rules will apply to both domestic and cross-border transfers of data."*

--- From [36]

4.3.3 Open Data Initiatives

Governments are increasingly making data about public services, including spending information, openly available online. Efforts of this kind include the Open Data Initiative [37] and the UK Government's similarly named initiative [38].

This is expected to have an impact on what types of data are available for processing in the cloud; for example, open data will affect medical research, enabling cloud services that perform data mining of public healthcare data.

Open data is an effort to increase accountability of public-sector officials and others in the public eye. For A4Cloud the relevance of open data is significant, as the project is investigating and implementing accountability mechanisms, especially for cloud environments – and it is cloud environments that will best serve the need to store and process massive databases of open data.

4.4 Standards

We identify next two sets of standards that A4Cloud ought to pay attention to – one set is the International Standardisation Organisation's security control standards, which apply worldwide, the other set is relevant only in the USA.

4.4.1 ISO 27017 / 27018

The existing ISO/IEC 27002 security control standards were developed in the pre-cloud era, and will be supplemented by the forthcoming **ISO 27017** ("Code of practice for information security controls for cloud computing services based on ISO/IEC 27002"). At the time of writing, ISO 27017 is at the end of the 'preparatory stage' (code 20.99 of the International Harmonized Stage Codes) so has still much iteration before it is approved and completed.

The forthcoming standard ISO 27018 ("Code of practice for data protection controls for public cloud computing services") is still in the preparatory stage, and focuses specifically on data protection aspects. It is however at a much more advanced stage of development and is expected to reach stable public draft by early 2014.

Since accountability is a notion that applies directly to the data protection context, it is important that accountability as a concept, and as a set of practices, is adopted or at the very least included in these standards. A4Cloud will need to monitor and participate in ISO activities when there is opportunity.

4.4.2 Fed RAMP and NIST

The US government has adopted the so-called Federal Risk and Authorization Management Program (Fed RAMP******) for the formal and ongoing evaluation of cloud service providers. Fed RAMP defines a set of criteria that public cloud service providers must meet in order to be approved for government use; so far the only cloud service provider that has full approval ('Authority to Operate') under the Fed RAMP program is Amazon Web Services – in particular, for its AWS East/West Regions IaaS service and its AWS GovCloud IaaS service††††††.

While A4Cloud is not specifically targeting government cloud services, the expectations of governments are important to take into account when building the reference architecture – or at least during the design stages – so that, if necessary, platforms developed by the project can be extended to meet needs such as those of governments without requiring massive re-engineering.

4.5 Technology

In 2010, the Internet had 2 billion connected users. The estimate for 2020 is that we will reach 5 billion internet users [39]. The demand for data processing in the cloud will be multiplied by a factor many times bigger than the increase in the number of internet users: in the future, ubiquitous computing will generate much more data than today's interconnected devices (there will be 50 billion devices online in 2020 [40]), representing a data explosion that can only be viable with the help of the cloud. Cloud accountability is fundamental to address most of the risks to personal and business data in an ethical way. Accountability can provide control and confidence to individuals, companies, governments, and other organisations on how this data is being handled in the cloud. In the following sections, we will discuss how technology trends will influence accountability in the cloud.

4.5.1 Ubiquitous Computing

The miniaturization of electronic devices, enabled by the innovation in materials and manufacturing processes, will make the internet of things explode (it already is growing at a very rapid rate with the almost universal adoption of smartphones, which include several interconnected sensors). The user interface will not be a cloud application, but everything behind it, as far as personal data is involved will involve the cloud.
The explosion of RFIDs and sensors, but also of consumer applications of many kinds of sensors (e.g. to monitor one's house), together with the emergence of wearable computing, will represent a huge challenge for privacy enhancing technologies and to accountability. In the same trend, interfaces with biological systems will allow to monitor individual's health indicators at real time [41]. Many applica-

****** See http://www.gsa.gov/portal/category/102375
†††††† See http://aws.amazon.com/govcloud-us/

tions will be deeply immersive, such as shopping experiences, learning, health care, and entertainment systems. They will be integrated to people's physical environment, in their clothes, and bodies. Google Glass‡‡‡‡‡‡ has emerged as an intriguing and powerful form of wearable computing. Applications will be available at any time and everywhere, making use of cloud computing resources to their maximum potential, but building on these small, cheap, fast devices to interconnect things and people.

A4Cloud needs to anticipate the concerns to accountability and privacy the use of, sensors, biosensors, and wearable computing will bring, and to foresee solutions for these questions. This underlines the importance of the Business Use Case 1: Health Care Services in the Cloud, being developed in the project, for instance.

4.5.2 Advances in Computing Power

There are on-going discussions on the validity of Moore's law in the coming years [42], but some recent results in 3D transistors by Intel may indicate that it is still safe for some more years [43]. The growth in computing power will continue to trigger paradigm shifts. When mobile phones started to have almost as much raw power to process data as PCs, the potential of mobile computing power was realised and opened new possibilities.

In the same way, advances in DRAM manufacturing and in-memory computing, are creating opportunities to perform parallel processing huge amounts of data, bringing big data into everyday business operations in many organizations, making big data scenarios a reality. Gartner says "The execution of certain-types of hours-long batch processes can be squeezed into minutes or even seconds allowing these processes to be provided in the form of real-time or near real-time services that can be delivered to internal or external users in the form of cloud services" [44]. As a technology trend, in-memory computing can bring difficulties in the justification of rightful processing of personal data, for instance, as business may collect and correlate personal data very rapidly, escaping notice unless suitable measures are taken. We can imagine that personal data records can be correlated with data coming from other sources (e.g. unstructured data from social networks, NO-SQL databases [45], and the like), then analysed in memory, for supporting a number of business decisions, and finally cleared out from the in memory database, for which no resilient trace would be found.

4.5.3 Advances in Security Research

There a number of security research topics that can influence the results of A4Cloud.

In cryptography, Homomorphic encryption and related techniques for performing operations over encrypted data [48, 49, and 50] allow in principle to move sensitive data even to less trusted cloud providers, since the confidentiality of the data would be preserved. These cryptographic schemes currently involve heavy computations, making its immediate exploitability difficult. The potential for breakthrough results in this area is noticeable, as there is market pressure for advancing the state of the art. The benefits are multiple, as risks for unauthorized data access are lowered. However this does not exempts cloud service providers from their accountability for the data stored in the cloud. Demonstrating capacity for correct handling of the (encrypted) data will still be relevant – data loss may cause harm to businesses and individual, even though the impact to the confidentiality will be minimized. Format-preserving encryption and data obfuscation are directly relevant and their implications need to be considered.

Concerning privacy enhancing technologies, we can mention static and dynamic data masking Technologies, for which there is an emerging market. The vendors in this sector had revenues around $100 million in 2011 and about $130 million in 2012 [51]. These techniques are being used to protect data at rest, to mask sensitive items in unstructured content, as in the redaction of reports, but also dynamically protect production data during operational accesses. They are mostly used by the enterprises' GRC departments, as a consequence of recommendations by regulatory mandates, such as PCI DSS and HIPAA. These techniques will become more relevant as the cloud adoption will progress, and it will be important to understand how data masking techniques can support accountability,

‡‡‡‡‡‡ See www.google.com/glass/start

and also to evaluate the reliability of the available tools and techniques with respect to the cloud accountability requirements.

5 Analysis

The key insights gleaned from analysing the data and reports cited in previous sections are summarised below, and here we take into consideration both the advances identified in section 3 and the groupings of trends discussed in section 4.

Cloud Services Market

The cloud services market is growing rapidly. The significance of creating and maintaining secure cloud services cannot be underestimated in the face of such growth.

There is growing emphasis on appropriate handling by service providers of common threats across different platforms. In order to thwart attacks and prevent the spreading of viruses, worms and hijacking of infrastructure, cloud service provider need to cooperate and share attack information.

There is widespread agreement that common data formats and protocols need to be adopted by cloud service providers, in order to achieve better interoperability. There are many ongoing activities in different organisations to agree on standards.

End Users, Privacy Assurance, Transparent Security

As we have concluded from the various studies cited in sections 3 and 4, for end users, the security (confidentiality, integrity and availability) of data stored in cloud computing services remains the foremost concern.

End users are very concerned about their privacy and individual freedom, and increasingly worried about how surveillance and the ease with which data in the cloud can be processed en masse may affect their personal lives; recent developments, such as the recently disclosed PRISM programme of the US government, are likely to reinforce these concerns. Cloud service providers will need to be more transparent about their practices and will have to work hard to achieve compliance with privacy laws and regulations.

Regulatory Initiatives, Management and Governance, Risk Assessment

The uncertainty of the legal framework for data protection in the EU is a major issue for cloud service providers. Building mechanisms and tools for better data governance is a key concern, and risk assessment methods that are suitable for cloud computing scenarios are in great demand and will continue to be in the near future.

Standards, Reference Architectures, Interoperable Governance

There is a major trend in development of cloud standards, with a long list of standardisation bodies participating in such activities. Only a few of these are widely adopted and there is still fragmentation in the cloud standards space and much competition between agencies. The demand for interoperability between different cloud service providers drives much of the standardisation work. There is also ongoing work on cloud computing reference models that incorporate appropriate security and privacy controls. Deliverable D:C-3.1 contains the project's most up-to-date analysis of standardisation activities.

Technology Trends

There is an unsurprising trend towards faster machines, implying an increasing capability to quickly process vast quantities of data; on the other hand, new encryption methods are on the rise, with homomorphic encryption standing out as a radically new technique that could revolutionise the way data is processed in the cloud. It remains to be seen whether homomorphic encryption can be implemented efficiently in practice. Other technologies to watch include format-preserving encryption and data obfuscation.

Other Issues

It is worth noting that developments such as the discovery of the PRISM programme raise important issues relevant to A4Cloud, but these are actually beyond the scope of the project. Government surveillance is a political issue that is not within the remit of our research work.

6 Conclusions

In this report we have identified a number of changes and trends that are relevant to the research within A4Cloud. Several 'hot topics' and developments have been listed, with extensive references to the current literature in the field.

We believe that the constant growth of the cloud computing services market will drive the need for better compliance and, hopefully, stronger privacy protection, as embodied in A4Cloud's notion of accountability. Of the developments identified here, we feel it is of paramount importance to track the amendments proposed to the EU's General Data Protection Regulation, and to monitor the potential impact of these until its eventual ratification by the European Parliament. Also the growing number of cloud computing standards needs to be carefully monitored, and we need to ensure that A4Cloud's reference architecture takes into consideration existing proposals, such as NIST's recently released security architecture for such architectures while filling important gaps. Emerging methods for risk assessment and privacy impact assessment need to be studied and monitored, as there is both a gap and an opportunity for a significant contribution for A4Cloud here.

The Project Horizons working group in A4Cloud will continue to actively monitor developments in the field and revisit the topics identified so far in a future report.

7 References

[1] Shams Zawoad, Amit Kumar Dutta, and Ragib Hasan. 2013. SecLaaS: secure logging-as-a-service for cloud forensics. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security (ASIA CCS '13). ACM, New York, NY, USA, 219-230.
[2] https://cloudsecurityalliance.org/research/grc-stack/
[3] http://www.gartner.com/newsroom/id/2220715
[4] http://www.gartner.com/newsroom/id/2163616
[5] http://www.idc.com/getdoc.jsp?containerId=prIT23744212#.UWJ-qVdI20p
[6] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/quantitative_estimates.pdf
[7] http://www.gartner.com/newsroom/id/2156915
[8] Top 100 Cloud Services Providers (CSPs) List And Research: http://talkincloud.com/tc100
[9] Top 10 cloud computing providers 2012: http://searchcloudcomputing.techtarget.com/photostory/2240149038/Top-10-cloud-providers-of-2012/1/Introduction
[10] http://ichitect.com/best-cloud/
[11] http://www.cloudxl.com/
[12] Citrix Vendor Landscape: Cloud Management Solutions: http://www.citrix.com/content/dam/citrix/en_us/documents/products/info-tech_research_group_cloud_management_vendor_landscape.pdf
[13] http://www.vmware.com/files/pdf/cloud/VMware-Taneja-Group-An-Overview-Of-The-Cloud-Market.pdf
[14] http://blog.dimensiondata.com/2012/10/dimension-data-is-positioned-as-a-leader-in-gartners-magic-quadrant-for-cloud-iaas/
[15] The Cloud Circa 2017: Services, Apps, Mobility: http://channelnomics.com/2012/08/17/cloud-competition-reshape-landscape/
[16] EC SWD(2012) 271 final: Unleashing the Potential of Cloud Computing in Europe http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf
[17] Critical Cloud Computing", A CIIP perspective on cloud computing services Version 1.0, December 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing

[18] ENISA threat landscape: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape
[19] McAfee Report “State of Security 2012”: http://www.mcafee.com/us/resources/white-papers/wp-state-of-security.pdf
[20] Involving Intermediaries in Cyber-security Awareness Raising: http://www.enisa.europa.eu/activities/cert/security-month/eu-u.s.-event-on-intermediaries-in-cybersecurity-awareness-raising/involving-intermediaries-in-cyber-security-awareness-raising
[21] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf
[22] PwC report, Changing the game - Key findings from The Global State of Information Security® Survey 2013, http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013-giss-report.pdf
[23] NIST - What is Special about Cloud Security: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910569
[24] NIST - ITL Bulletin for June 2012, Cloud Computing: A Review of Features, Benefits, and Risks, and Recommendations for Secure, Efficient Implementations: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911668
[25] NIST - Cloud Computing Synopsis and Recommendations: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075
[26] http://blog.fixya.com/pr/nov2012/cloud-storage-report.html
[27] http://www.zdnet.com/dropbox-gets-hacked-again-7000001928/
[28] http://www.idc.com/getdoc.jsp?containerId=prUK23748512
[29] https://www.eff.org/deeplinks/2012/01/department-justice-misdirection-cloud-computing-and-privacy
[30] http://gizmodo.com/5932161/why-the-cloud-sucks
[31] http://www.networkworld.com/news/2012/080912-cloud-computing-debate-261518.html
[32] http://europe-v-facebook.org/EN/en.html
[33] http://edri.org/edrigram/number11.10/privacy-dpa-irish-facebook-case
[34] Loeb & Loeb LLP, “United States: The EU’s Cloud Computing Initiative”. Article available at http://www.mondaq.com/unitedstates/x/213212/Data+Protection+Privacy/The+EUs+Cloud+Computing+Initiative
[35] European Commission, “Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions: Unleashing the Potential of Cloud Computing in Europe”, Copy available at http://www.loeb.com/files/Uploads/EU_Cloud.pdf
[36] http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en
[37] http://www.opendatainitiative.org
[38] http://www.computerworlduk.com/news/public-sector/3321660/osborne-announces-open-data-initiative/ and http://data.gov.uk/
[39] http://www.pcworld.com/article/185768/10_ways_the_internet_will_change_in_2010.html
[40] http://www.telegraph.co.uk/technology/internet/9051590/50-billion-devices-online-by-2020.html
[41] http://blogs.discovermagazine.com/sciencenotfiction/2010/08/20/wifi-medicine-implantable-biosensors-that-could-email-your-doctor/#.UZnoCLV_Pzw
[42] http://techland.time.com/2012/05/01/the-collapse-of-moores-law-physicist-says-its-already-happening/
[43] http://www.bbc.co.uk/news/technology-17785464
[44] http://www.gartner.com/newsroom/id/2209615
[45] http://www.techrepublic.com/blog/10things/10-things-you-should-know-about-nosql-databases/1772
[46] http://research.google.com/archive/bigtable.html
[47] http://research.google.com/archive/mapreduce.html
[48] http://cacm.acm.org/magazines/2010/3/76272-computing-arbitrary-functions-of-encrypted-data/fulltext
[49] Seny Kamara, Charalampos Papamanthou, Tom Roeder, Dynamic Searchable Symmetric Encryption, in ACM Conference on Computer and Communications Security (CCS '12), October 2012
[50] Florian Kerschbaum: Outsourced private set intersection using homomorphic encryption. ASIACCS 2012: 85-86.
[51] http://www.gartner.com/technology/reprints.do?id=1-1DCIUZJ&ct=121224&st=sb
[52] http://www.renewableenergymagazine.com/article/cloud-computing-has-a-silver-lining

[53] http://www.accenture.com/us-en/Pages/insight-environmental-benefits-moving-cloud.aspx
[54] https://openhpi.de/course/inmemorydatabases
[55] http://www.wired.com/wiredenterprise/2012/05/apple_coal/
[56] Yu, Q.; Liu, Y.; Chen, T.P.; Liu, Z.; Yu, Y. F.; Lei, H. W.; Zhu, J.; Fung, S., "Flexible Write-Once–Read-Many-Times Memory Device Based on a Nickel Oxide Thin Film," *Electron Devices, IEEE Transactions on*, vol.59, no.3, pp.858,862, March 2012
[57] S. Sundareswaran, “Ensuring Distributed Accountability for Data Sharing in the Cloud,” *Dependable and Secure Computing*, vol. 9, 2012.
[58] C. Wang and Y. Zhou, “A collaborative monitoring mechanism for making a multitenant platform accountable,” in *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing*, Berkeley, CA, USA, 2010, pp. 18–18.