D1.1.3

Exploitation Roadmap

Project number:	257243
Project acronym:	TClouds
Project title:	Trustworthy Clouds - Privacy and Resilience for Internet-scale Critical Infrastructure
Start date of the project:	October 1st, 2010
Duration:	36 months
Programme:	FP7 IP

Deliverable type:	Report
Deliverable reference number:	ICT-257243 / D1.1.3 / 1.0
Activity and Work package contributing to the deliverable:	Activity 1 / WP 1.1
Due date:	December 2010 – M03
Actual submission date:	23rd December 2010

Responsible organisation:	UMM
Authors:	UMM (Ruediger Glott, Kirsten Haaland, Andreas Meiszner); HSR (Marco Nalin, Ilaria Baroni); OXFD (Imad Abbadi); PHI (Milan Petkovic); EDP (Miguel Areias); IBM (Elmar Husmann)
Dissemination level:	Public
Revision:	1.0

Abstract:	This document provides a roadmap for the exploit-tation of the TClouds infrastructure. It starts from the two ICT scenarios in which TClouds will be developed and tested during the project phase, home health care and public lighting, and identifies possible starting points for the implementtation of the TClouds infrastructure in other ICT and business scenarios. The content of this roadmap will be checked for consistency with market and technology trends throughout the project period, updates of the baseline information provided in this roadmap will be included in other deliverables of Activity 1.
Keywords:	Cloud computing, business models, roadmapping

Table of Contents

List of figures

1 Introduction

The vision of TClouds is to contribute to a Future Internet where federations of standardised resilient and privacy-protecting global infrastructure clouds offer virtualised computing, communication, and storage resources that allows hosting of critical and non-critical ICT systems. On the one hand, the realisation of this vision requires successful showcases to be provided by the TClouds consortium and innovations at the level of software components and open standards to enrich cloud technology frameworks with federated trust and security capabilities. On the other hand, in order to achieve a significant uptake of the opportunities provided by TClouds by other commercial and non-commercial actors, these potential users need a form of guideline on how the TClouds assets (principles, policies, security extensions at software component level, open cloud standards) can be used in a most effective way in different scenarios. This also needs to tie in with complementary Future Internet research in Europe that work on other elements of the federated cloud infrastructure vision such as the FP7 projects RESERVOIR (federated virtual computing), VISION (federated virtual storage) or SAIL (federated virtual networks).

This document provides a roadmap for the exploitation of the TClouds assets. While exploitation roadmaps usually support the management of the activities and tasks required to deliver the needed capability through equipment programmes or other lines of development, this roadmap has a more limited scope because the TClouds project – as an advanced research project - aims only at prototyping of the federated cloud computing infrastructure within two usage scenarios. Therefore, this roadmap starts from the two ICT scenarios in which TClouds will be developed and tested during the project phase, home health care and public lighting, and identifies possible starting points for the implementation of the TClouds infrastructure in other ICT and business scenarios.

Regarding the character and purpose of this project, it must be noted that “roadmapping is a strategic planning process which helps to align and communicate the business need (Know Why), with the delivery programmes (Know What) and the underpinning resources (Know How).”[1] Roadmaps must not be confused with project plans, as their timeframe usually exceeds the project period, as they deal with more strategic levels of information, and as they are often concerned with navigating through areas of high uncertainty.[2] The above-mentioned uncertainty pertains particularly to the sectors and concrete usage cases in which companies and other actors may take up and implement the TClouds infrastructure in future. Therefore, this roadmap must remain preliminary to a certain degree, and checked throughout the whole project period for consistency with actual developments within as well as outside the TClouds project. To this end, the various outcomes of Activity 1 of the TClouds project will refer to this roadmap as a baseline and update the information provided in this document in other deliverables of A1 whenever necessary and possible.

The remainder of this deliverable is structured as follows: In the next section, we describe the framework and scope of the exploitation roadmap. This section is divided into three sub-sections. First, we illustrate the global trend towards cloud computing and the driving forces behind this development.

In the second part, we discuss the barriers that might hinder tapping the full potential provided by cloud computing. The third part of section 2 provides an overview of current business practices regarding cloud computing. This sub-section will be subject to the aforementioned checks and updates of the information provided in this roadmap in later deliverables of A1.

[1] Institute for Manufacturing (IfM) of the University of Cambridge, 2006: Technology Roadmapping Guidance. Cambridge. Available online at: http://www.ifm.eng.cam.ac.uk/ctm/trm/documents/-mod_trm_v1_1.pdf

[2] Ibid.

In the third section, we discuss the exploitation requirements that derive from the market situation and illustrate how TClouds will address these points. This section refers to the exploitation of the TClouds platform that is developed in TClouds' Activity 2 and to the prototypes developed for two usage scenarios in Activity 3.

The final section will be provided by the graphic visualisation of the exploitation roadmap for TClouds.

2 Framework of the Exploitation Roadmap

2.1 The global trend towards Cloud Computing

The exploitation of the TClouds infrastructure depends largely on the overall trends in the market for cloud computing. Kim (2009)[3] probably describes this market situation best: "Cloud computing is in its infancy in terms of market adoption. However, it is a key IT megatrend that will take root." There is a widespread belief in vast market opportunities for cloud computing. According to a report of the Centre for Economics and Business Research (CEBR), the widespread adoption of cloud computing could give the top five EU economies (Germany, France, UK, Italy and Spain) a boost of 763 billion Euro and 2.4 million jobs until 2015.[4]

According to the CEBR report, which was commissioned by EMC, a data storage and IT solutions firm that provides cloud computing services, the adoption rates of private, public and hybrid clouds will raise from around 32% to 37% (Spain) in 2010 (see Figure 1) to 45% to 56% in 2015 (Figure 2). It must be noted, however, that other surveys show much lower actual adoption rates, though. For instance, in 2009 IDC found that only 7% of the German firms used already cloud computing.[5] We assume that there are different methodologies behind these differences, for instance, whether or not using cloud-based email services or search engines falls within a study's definition of cloud computing results in a very significant difference of the share of cloud usage.

Country	Current adoption rates (private, public and hybrid)
United Kingdom	32%
Germany	33%
France	31%
Italy	32%
Spain	37%

Source: IDC 2010 European Services Survey, Cebr analysis

Figure 1: Current unweighted average adoption rates by country[6]

[3] Kim, W., 2009. Cloud computing – today and tomorrow. Journal of Object Technology, Volume 8, No. 1, 2009; pp. 65-72. Available online at: http://www.jot.fm/issues/issue_2009_01/column4.pdf

[4] See EMC, 2010. The Cloud Dividend. Available online at http://uk.emc.com/microsites/2010/cloud-dividend/index.htm; Weber, T, 2010. Cloud computing 'could give EU 763bn-euro boost' Available online at: http://www.bbc.co.uk/news/business-11931841; ChannelPartner, 2010. Analyse: Cloud-Markt in D. Available online at: http://www.channelpartner.de/channelcentre/cloud_computing/298369/

[5] IDC, 2009. IDC Focus: Cloud Computing ist in Deutschland noch nicht angekommen. Available online at: http://www.t-systems.de/tsi/servlet/contentblob/t-systems.de/de/873440/blobBinary/09-06_Cloud-Computing-ps.pdf

[6] Figure copied from Channel Partner, 2010: Analyse: Cloud-Markt in D. Available online at http://www.channelpartner.de/channelcentre/cloud_computing/298369/

Country	Prospective adoption rates (private, public and hybrid)
United Kingdom	56%
Germany	45%
France	48%
Italy	51%
Spain	51%

Source: IDC 2010 European Services Survey, Cebr analysis

Figure 2: Prospective unweighted average adoption rates by country[7]

This trend is expected to go along with a rapid growth of new businesses in the five EU Member States (Figure 3), and the creation of 2.4 million jobs.

Country	New business start-ups
United Kingdom	35,000
Germany	39,000
France	48,000
Italy	81,000
Spain	55,000

Source: Etro (2009)

Figure 3: New business start-ups by 2015[8]

The report identifies mainly four benefits cloud computing generates for businesses (Figure 4):

- Business development opportunities are expected to contribute about 15% of all cloud-induced benefits to businesses in France, Germany, Italy and Spain. In the UK, the relative share of this benefit is expected to be about 25% in 2015.
- The generation of new businesses is expected to make up about 30% of all cloud-based benefits in France, Germany, Italy and Spain, but only 15% in the UK.
- The relative share of net cost savings through cloud computing is expected to reach 15%-20% within the five countries.
- Multiplier effects through cloud computing play the strongest role, as their relative share is expected to be about 35% in all five countries.

[7] Figure copied from Channel Partner, 2010: Analyse: Cloud-Markt in D. Available online at http://www.channelpartner.de/channelcentre/cloud_computing/298369/

[8] Figure copied from Channel Partner, 2010: Analyse: Cloud-Markt in D. Available online at http://www.channelpartner.de/channelcentre/cloud_computing/298369/

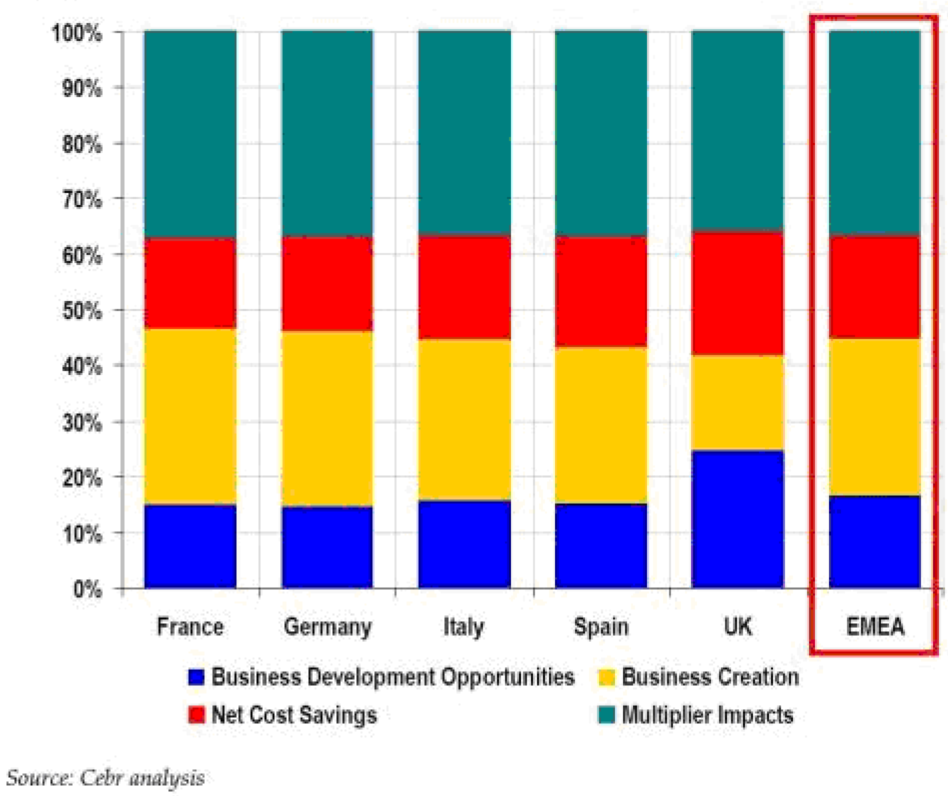

Figure 4: Percentage contributions of the individual categories of the cloud computing benefits, EMEA and individual countries[9]

Experts identify four key drivers that accelerate the cloud adoption rate in Europe. One factor is that the available technology has improved with regard to connectivity, internet speed and virtualisation technologies, which make the use of servers more efficient.[10]

The second factor is the emergence of new business models that are characterised by an "as-you-consume" pricing strategy instead of the overcome and often expensive lump sums for software licences. [11] For instance, ParaScale, a US-based storage service provider, planned to charge its clients between $1 and $1.50 per gigabyte when using its software and hardware. The monthly rate for cloud storage services would be $0.15 per gigabyte. Foley (2008) claims that with such low fees ParaScale would pay for itself in 10 months in a corporate data centre.[12] According to Kim (2010)[13], Amazon charges 15 cents a month per gigabyte of S3 storage, 10 to 80 cents per hour for EC2 server, and offers a 10% credit if S3 availability falls below 99.9% in any month.

[9] Figure copied from Channel Partner, 2010: Analyse: Cloud-Markt in D. Available online at http://www.channelpartner.de/channelcentre/cloud_computing/298369/

[10] Weber, T, 2010. Cloud computing 'could give EU 763bn-euro boost' Available online at: http://www.bbc.co.uk/news/business-11931841

[11] Ibid.

[12] Foley, J., 2008. 20 Cloud Computing Startups You Should Know. Available online at http://www.informationweek.com/news/cloud-computing/software/¬showArticle.jhtml?articleID-=210602537

[13] Kim, W., 2009. Cloud computing – today and tomorrow. Journal of Object Technology, Volume 8, No. 1, 2009; pp. 65-72. Available online at: http://www.jot.fm/issues/issue_2009_01/column4.pdf

The third factor is consumerisation of IT, which largely refers to the seminal trend towards mobile computing. In this context, cloud computing offers companies a competitive edge. [14] Indeed, as Pemmaraju & Rangaswami (2010)[15] report, business agility together with cost efficiency provide by far the most important reasons for companies to move towards cloud computing. Another driver of cloud computing is that the cloud can be accessed anytime from anywhere, which is a key factor for mobile and flexible use.[16]

Cloud computing replaces big up-front costs that have been usual for IT investment through a continuing operating expenditure that rises and falls with demand. Interestingly, the cost efficiency argument gained power only recently during the economic crisis. Until then, it seems, have the security risks aligned with cloud computing dominated over the potential cost savings.[17]

2.2 Barriers towards cloud computing

Pitfalls for the adoption of cloud computing, besides the still existing security risks, are seen in the lack of user friendliness that is aligned with many cloud computing offerings and the cultural change that is demanded from a company when moving towards cloud computing.[18]

Kim (2009)[19] sees a number of problems that must be solved in order to tap the potentials cloud computing offers. The first problem he discusses is availability, which is a topic triggered by outages of the Amazon S3, Google Gmail, Citrix's GoToMeeting and GoToWebinar and RIM's BlackBerry service in 2008. Despite these outages, Kim assumes that availability is not a severe problem for cloud computing, as he estimates that the availability of cloud services is higher than 99% and thus comparable to on-premises availability.

Security and privacy issues, the second problem Kim discusses, is considered by him to be a generic threat to IT infrastructures and thus not cloud-specific. He points out that "it is nearly impossible to guarantee 100% security and privacy protection against all possible sources of violation, including the inevitable software bugs, the growing sophistication of the hackers, inadequate procedures, human malfeasance, and human errors." He concludes that for cloud computing vendors there is nothing else for it but to adopt the most sophisticated and up-to-date tools and procedures and to strive to provide better security and privacy than is available for on-premises computing.

However, other studies do see a number of severe risks, of which some appear bigger than in other IT environments, when a firm outsources its IT infrastructure to a cloud. For instance, Gartner (2008)[20] discusses the problem of "Privileged User Access" in cloud environments. If sensitive data is processed outside the enterprise and handled by employees of the cloud provider, special care has to be taken to control who has access to the data and how to

---

[14] Weber, T, 2010. Cloud computing 'could give EU 763bn-euro boost' Available online at: http://www.bbc.co.uk/news/business-11931841

[15] Pemmaraju, K. & Rangaswami, M. R., 2010. Leaders in the Cloud. Identifying the Business Value of Cloud Computing for Customers and Vendors. Available online at: http://createyournextcustomer.-techweb.com/wordpress/wp-content/uploads/2010/04/cloud-survey-findings.pdf

[16] Kim, W., 2009. Cloud computing – today and tomorrow. Journal of Object Technology, Volume 8, No. 1, 2009; pp. 65-72. Available online at: http://www.jot.fm/issues/issue_2009_01/column4.pdf

[17] Weber, T, 2010. Cloud computing 'could give EU 763bn-euro boost' Available online at: http://www.bbc.co.uk/news/business-11931841

[18] Ibid.

[19] Kim, W., 2009. Cloud computing – today and tomorrow. Journal of Object Technology, Volume 8, No. 1, 2009; pp. 65-72. Available online at: http://www.jot.fm/issues/issue_2009_01/column4.pdf

[20] Brodkin, J., 2008: Gartner: Seven cloud-computing security risks. Available online at http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

ensure the trustworthiness of these people. ENISA (2009)[21] discusses the problem of "Loss of Governance". The customer cedes control over security issues to the Cloud Provider, which may not be not be covered by a commitment in the service level agreement. Both, ENISA (2009) and CSA (2010)[22] discuss the problem of "Malicious Insiders". The damage that may be caused by a malicious insider is great, especially in the case of system administrators or security service providers. CSA points out, in this regard, that due to convergence of IT services and customers on a single management domain the threat of malicious insiders is amplified. Moreover, the processes and procedures within the cloud providers may not be transparent to the customers.

Kim points out that support for problem resolution is indeed an issue at current, as free SaaS cloud users are often left alone. For enterprises, the situation is not as problematic because companies pay for support. However, high quality support that is competitive to on-premises computing requires from cloud computing vendors to hire and train adequate support staff. Kim recommends designing cloud services for easier usability than on-premises computing.

Another aspect Kim discusses is the role of vendor lock-ins and interoperability issues as pitfalls for cloud computing business. Though all actors in the market have learned to live with vendor lock-ins he claims that interoperability and open standards would help significantly to counter this risk. However, he observes that interoperability has not yet received the attention it deserves, which he assumes to be due to the infancy of the market for cloud computing.

Finally, Kim discusses compliance issues, as commercial users must maintain business legal documents and assure their integrity in order to comply with laws. This might pose a challenge to cloud computing vendors since they have to ensure that their enterprise users' data satisfy their compliance requirements. Like interoperability issues, this concern has not received the attention that should be paid to it, according to Kim.

The TClouds project shares the assumption that cloud computing creates specific security challenges in addition to the security challenges posed by traditional ways of IT hosting. In particular, the federated (cloud-of-clouds) cloud approach further intensifies some of the issues raised above. In a federated cloud environment, the allocation of virtual resources may i.e. be dynamically spread across multiple administrative domains and cloud providers.

This has also legal and regulatory implications as typically the contractual relation will be between the customer and a single cloud provider whereas the cloud services are provided by a federation of providers. This mirrors i.e. today's interaction with Internet Service Providers (ISPs).

[21] European Network and Information Security Agency (ENISA), 2009. Cloud Computing - Benefits, risks and recommendations for information security. Available online at: http://www.enisa.europa.eu/-act/rm/files/deliverables/cloud-computing-risk-assessment

[22] Cloud Security Alliance (CSA), 2010. Top Threats to Cloud Computing V1.0. Available online at: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

2.3 Cloud computing – business examples

Cloud computing is much more than SaaS or simple storage, and it is also more than just another IT outsourcing strategy. Figure 5 shows the services that are possible to create and offer in the three basic forms in which cloud computing can be performed (IaaS, PaaS and SaaS).

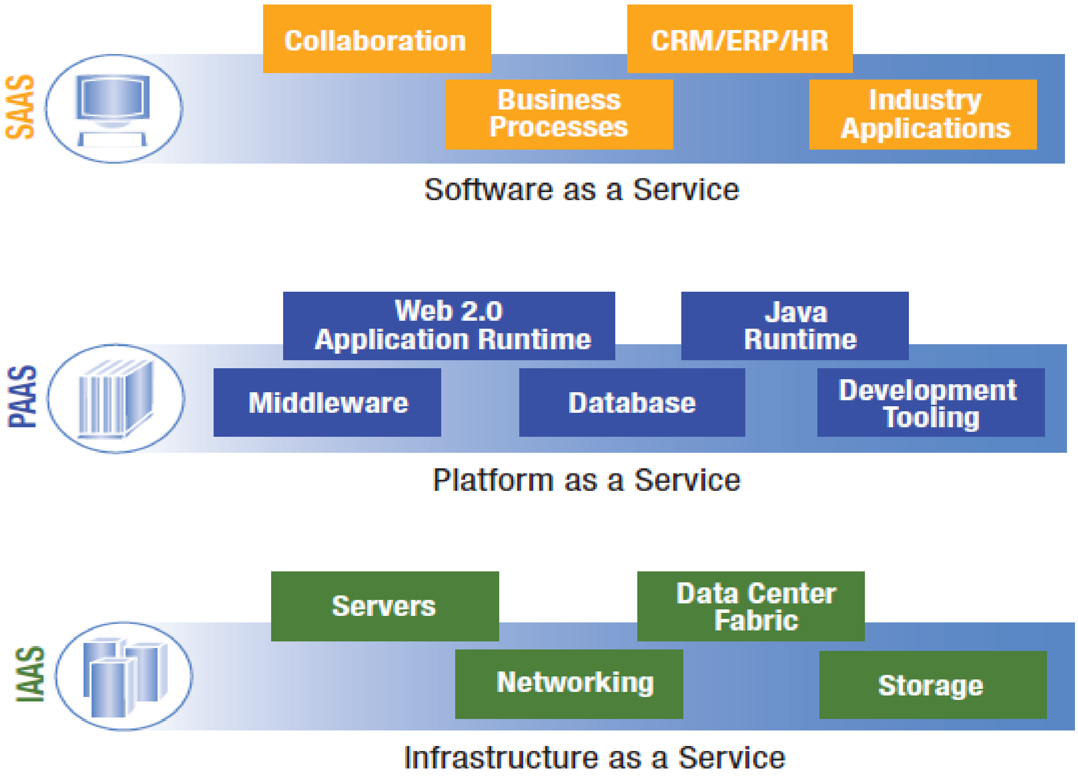

Figure 5: Cloud computing and service offerings[23]

Overall, cloud-related services can be categorised as follows (Knorr & Gruman 2008, Foley 2008)[24]:

- **Software as a Service (SaaS)** means to run a single application in a data centre, and deliver the functionality via the Internet to the users. Examples of enterprise SaaS vendors are Salesforce.com (for sales force applications), Oracle/Siebel (CRM applications), Workday (for ERP applications), Citrix (meeting applications). Examples of SaaS desktop applications for end users are Google Apps, Zoho Office, Microsoft WindowsLive, etc. Finally, Internet portal sites, Internet search engines, and Internet social networking sites are essentially SaaS vendors for end customers.
- A more restricted sub-type of SaaS are Internet platforms that offer *Web services* - specific APIs that application developers can use in developing applications that

[23] Schunter, M., 2010. IT Sicherheit und Cloud Computing. Zurich: IBM Research

[24] Knorr, E. & Gruman, G., 2008: What cloud computing really means. Available online at: http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031?page=0,0; Foley, J., 2008. 20 Cloud Computing Startups You Should Know. Available online at http://www.informationweek.com/news/cloud-computing/software/showArticle.jhtml?articleID-=210602537

integrate services of the platform. Examples are Google Maps, ADP payroll processing, the U.S. Postal Service, Bloomberg, credit-card processing services, etc.

- A similar sub-type of SaaS are *Managed Services*, such as virus-scanning services for email, spam-filtering services (Google/Postini, etc.), security services (SecureWorks, IBM, Verizon, etc.), desktop management services (CentreBeam, Everdream, etc.)
- **Platform as a service (PaaS)** delivers an application development environment (platform) as a service, usually also equipped with computing resources for hosting the applications developed on the platform. Examples are Amazon, Salesforce.com (Force.com), Coghead, Google (Google App Engine), Yahoo (Pipes), and Dapper.net. The Amazon Web Services (AWS), which is an important platform for many SaaS startups, consist of Simple Storage Service (S3), Elastic Compute Cloud (EC2), Simple Queuing Service (which uses S3), and SimpleDB. Examples for startups operating on top of AWS are Desktop Two, Zimdesk, GOPC, and Sun Microsystems' Secure Global Desktop. Another example, a startup in this field, is provided by Skytap (http://www.skytap.com), which offers a platform for virtual software testing as an on-demand service. Users can choose from a variety of operating systems (Linux, Solaris, and Windows) and databases. Skytap's Virtual Lab supports testing software for function, performance, and quality assurance, and it can be used for preproduction staging.
- **Infrastructure as a Service (IaaS)** [25] means to offer computing resources in form of virtual servers and storage as utility computing service. Examples are Sun Microsystems, IBM, Amazon and AT&T; and new vendors such as Nirvanix, Hatsize, Joyent, Cloudworks,

It appears as if Kim's prognosis from beginning of 2009 has already been realised to quite an extent. Kim forecasted "ample room for hundreds or even thousands of players in the market" that will give opportunities to many "large clouds" and a lot more "small clouds". Many of the small clouds, so Kim, will benefit from the infrastructure offered by the large cloud providers, i.e. IaaS will likely become more important the more the market for cloud computing evolves.

As a result of the growing number of cloud-based services, Kim predicted the emergence of cloud technology integrators as a new form of cloud-based services. Firms like Kaavo, RightScale or CohesiveFT offer already such services[26].

The market dynamics, as foreseen by Kim, would further result in the emergence of a cloud computing ecosystem that includes different types of players. The first group would be provided by the vendors that offer cloud services to the users. A second type offers solutions that help enterprises to provision and manage virtual data centres from commodity servers and storage, (e.g. 3Tera (AppLogic), Cohesive FT (Elastic Server on Demand)) Another type offers solutions for deploying and managing applications in a data centre (within an enterprise). Examples for such service providers are Elastra and Maavo. "Other types of player will include cloud computing platform vendors, the usual application software and middleware vendors, system integrators, and consultancies" (Kim 2009).

Finally, according to Kim, the evolution of the cloud computing market and the demand for availability and security will result in a growing adoption of hybrid clouds, and as a result of more mature clouds and services in the future the fees users must pay for cloud computing resources and services will increase.

---

[25] Knorr & Gruman do not include IaaS in their classification, but what they call "utility computing" includes IaaS.

[26] Foley, J., 2008. 20 Cloud Computing Startups You Should Know. Available online at http://www.informationweek.com/news/cloud-computing/software/showArticle.jhtml?articleID-=210602537

3 Exploitation Requirements and the TClouds Approach

The aforementioned aspects of the market and prospects of cloud computing largely determine the requirements that must be met in order to exploit the TClouds infrastructure cloud.

Firstly, the vast growth that is predicted for the market for cloud computing hardware, software and services suggests that any cloud product can be successfully exploited and marketed in the near future. However, it must be taken into account that these positive outlooks are based on two driving forces that appear rather weak and ambiguous than promising: the economic crisis and the lack of experience of companies and individual cloud users with cloud infrastructures.

The economic crisis has obviously led to a fundamental re-evaluation of the importance businesses award to privacy and security risks on the one hand and to cost efficiency on the other hand. As long as the cost pressure continues, firms might go on valuing savings higher than security threats to their systems and their clients. However, if cost pressure decreases or if the lesser attention paid to security concerns results in a fundamental breakdown of a major cloud system or to a severe violation of privacy rights of a notable number of cloud users, the currently positive trend towards cloud computing might be affected.

Currently the cloud security market is developing in three major directions (from a security and privacy perspective):

- **Commodity/public clouds** – such as Amazon EC2 (IaaS) or Google Apps (PaaS) that offer cloud services at relatively limited degrees of security and privacy protection. Mostly these providers also defer reliabilities in their terms of use. So here the protection of security and privacy is largely in the hand of the customers. This has led to a number of complementary services that serve to add specific security elements to commodity clouds.
- **Highly secure private clouds** – that offer specific environments for a single customer where security is individually adapted to the needs of the customer. Due to the single tenant approach of private clouds – many of the security concerns of cloud computing can be circumvented. However, it is also a costly model where many of the potentials of cloud computing are not leveraged (such as i.e. effective sharing of resources).
- **Community clouds** – that bridge elements of commodity clouds with those of private clouds. I.e. IBM and Google have both launched in the US in 2010 specific IaaS and PaaS community clouds for governmental agencies that also comply to US federal security requirements (FISMA). Other examples are SaaS clouds for the health secture such as Microsoft’s Health Vault or Google Health.

The inexperience of many cloud users with cloud infrastructures is visible by the fact that large public cloud infrastructure providers, like Amazon or Google, offered their cloud infrastructure and services to users, and they found indeed significant demand, at a time when companies with the expert knowledge needed to manage and control these clouds from the user’s side were hardly existing. Hence, public clouds have primarily been used for non-critical applications. The general recognition of the advantages of cloud computing on the one hand and the increased recognition of security threats on the other hand has more recently fuelled the rise of private clouds and specific community clouds.

TClouds aims to create a similar level of security and privacy protection in a federated commodity/public cloud environment as it currently may only be realized in a private or specific community cloud – ultimately creating a *Virtual Private Cloud* on a public infrastructure. This supports the further convergence of ICT and supports that a federated cloud infrastructure could become the backbone of a Future Internet.

As laid out in the DoW of TClouds, the protection of critical infrastructures, such as communications, energy or healthcare, is an increasingly important task because these infrastructures become tremendously dependent on computer and network infrastructures. Also these critical infrastructures are so large-scale that it is almost impossible to cover them widely with a private or community cloud from a single provider. Further to this, dependency on single providers will further increase concerns about resilience. The simplification and commoditisation of ICT-supported services that is driven by cost pressures does also hold for such critical ICT infrastructures. Indeed, the continued push to outsource even critical ICT is exemplified by current efforts to leverage scalable shared computing, communication, and storage infrastructures that are provided by third party enterprises.

It must therefore be regarded as an open question how many of the firms using cloud services will possibly withdraw in the future or revert to highly-secure private clouds if they find out that they made serious mistakes when using a cloud, or if they just realise that their capacities to handle the cloud efficiently are limited and require additional services that must be paid for. Especially the expectation of some experts (e.g. Kim 2009) that fees will increase with the growing evolution of the market should be considered, in this regard.

It cannot be emphasised enough that virtually all experts claim that privacy and security issues of cloud computing still are not resolved. We consider this weakness as the key factor to be addressed when the vast potential attributed to cloud computing shall be realised. Other problems, such as availability and support, fall behind the significance of privacy and security, because availability of cloud services seems already to be provided at a comparable level as on-premise computing, and the dynamics of the market has allowed the emergence of numerous companies that offer the support cloud users need.

Thus, as a conclusion we maintain that the foundations for the move towards a cloud-based economy are set, as technology as well as services are mature enough and the market shows a dynamic strong enough to absorb the growing demand for cloud computing, in the long run. However, to tap this potential requires a solid solution of the privacy and security risks aligned with cloud computing. To this end, the exploitation strategy of TCLOUDS must meet the following requirements:

- TClouds must primarily aim at the sustainable resolution of privacy and security issues aligned with existing clouds and help creating general trust into cloud computing infrastructures
- The TClouds cloud must support vendor and platform independence, e.g. through open standards and interoperability
- The federated cloud developed by TClouds must help firms to meet compliance requirements at any point of the transactions that take place within the cloud.
- A federated cloud that is designed to be used on top (or around) other cloud systems and services – like the TClouds cloud - must be cost-efficient in order not to accelerate the expected price increase.
- Given the complexity of existent clouds, the TClouds cloud must be easy to understand and to use, so that any kind of user is capable to use the functionalities he wants, and to easily monitor and control the system in which his business processes are performed without significant time and financial effort.

The TClouds consortium considers the approach towards federated infrastructure clouds as a move in the right direction in order to address all these points. Federation at the IaaS level (virtual compute-, storage- and network-resources) is particular powerful as the provided services are highly similar. Cloud projects from the Internet of Services domain (such as RESERVOIR and VISION) have already demonstrated that federation across IaaS providers is technically feasible and may increase availability and scalability. However, security and privacy concerns provide the primary adoption hurdle to this cloud-of-clouds vision.

The following description of the TClouds approach is taken from the DoW in order to illustrate how TClouds addresses the requirements laid out above:

> TClouds technology will enable infrastructure providers to build scalable virtual infrastructures based on open standards that can be offered as a computing utility to a wide range of stakeholders. Furthermore, it will enable secure federation of standardised infrastructure clouds such that the trustworthiness of the overall system no longer depends on the trustworthiness of any individual part. This federated approach will guarantee that the infrastructure does not fail unless a substantial fraction of the providers fail.

A clear societal and business benefit is that we will enable even small players to use the TClouds platform to provide ICT services that guarantee privacy- and resilience that is mandatory for today's critical ICT applications. This provides the cost and scalability benefits of virtual infrastructures to a wider range of applications while at the same time strengthening their privacy and resilience.

The generic infrastructure cloud platform built by TClouds for piloting purposes will demonstrate adequate and cost-efficient means to secure virtualized and federated computing, storage, and network services. It will further be applied to the two use case areas of TClouds that showcase the needs of specific critical infrastructure domains.

The TClouds application domains are however not restricted to these cases and may range from common web-content distribution to hosting of any critical ICT services. As a consequence, we expect an ecosystem of SaaS or PaaS level cloud providers to emerge that adopt TClouds principles while delegating the infrastructure-level challenges to the emerging ecosystem of federated IaaS providers that use TClouds assets such as open standards or security extensions at the software component level.

Hence, the success of the TClouds exploitation may be measured by the level of adoption of TClouds assets (principles, policies, security extensions at software component level, open cloud standards) by the cloud market – whereas an exploitation of the TClouds platform build for the two pilot cases is not specifically intended.

An important property of the emerging cloud infrastructure will be that it respects global legal requirements, i.e., that unlike today's global infrastructures, TClouds technology will be regulation-aware, e.g., in the sense that it will ensure that data mobility is limited to ensure compliance with a wide range of different National legislations. For this reason it might be mandatory that some of the TClouds assets are used in combination. This will be clearly indicated in the TClouds principles and policies.

In order to enable this vision, we need already to ensure that certain core principles are satisfied:

- Federation of independent providers: One goal is to enable an ecosystem of independent providers. This will guarantee that the overall service does not depend on any individual provider.
- Flexible trust models: Trust models need to be flexible, i.e., users need to be able to determine what players and what mechanisms to trust. Another aspect is user-centric security and privacy policies, i.e., those stakeholders using cloud-based services, be they individuals, SMEs or other organisations, can determine their individual security and privacy preferences.
- Open interfaces: In order to foster the creation of an adequate ecosystem for critical applications, openness of the architecture and interfaces is essential. This will enable interoperation between different clouds as well as seamless migration of workloads while maintaining the given security constraints. TClouds will also base its work on the emerging open standards developments for infrastructure clouds and collaborate with the relevant standardisation groups such as the DMTF Open Clouds Standards Incubator, the SNIA Cloud Storage Technical Working Group or the OGF Open Clouds Computing Interface Working Group.

- Scalable security mechanisms: Our security extensions must not break the underlying cloud principles. This means that deployed mechanisms must be scalable and transparent and must be resilient to expected failures of the underlying virtual infrastructure.

This enables users to decide on their trust requirements and thus encourages user-centric deployment of appropriate security mechanisms that are trusted by an individual user.

4 The TClouds Scenarios – demonstrating Exploitation Possibilities

The development and the evaluation of the TClouds assets will be demonstrated through two significant use cases. These will help to check and demonstrate the capacities of TClouds for critical processes in significant usage areas, namely: home health care and energy supply.

The impact of a trusted infrastructure cloud on energy supply networks and processes provides the first scenario in which the capacity of the TClouds assets shall be tested and demonstrated. For this purpose, TClouds assets will be combined with a state-of-the-art federated cloud platform to form the TClouds experimental platform.

The first concrete use case that will serve as a test bed for TClouds is the smart provision of energy to municipal clients for their public lighting (Smart Lighting). The idea is to control the energy supply so that it can be aligned with actual demand, which can vary significantly from day to day or under changing conditions.

The actors involved in this scenario are:

- Operators (Municipalities, EDP)
- Clients (Municipalities)
- Administrators (EDP)

The business functions that are affected from the public lighting solution span a wide range, as they include the monitoring of consumption and of state and anomaly events (alarms), the management of lighting services and schedules, of Public Lighting settings and of settings of Public Lighting Intelligent Devices (DTC & EB), and the actuation over Control Circuits. The use cases that were defined for this scenario are:

- Operation & Control
- Alarm Management
- Change Service / Schedule
- Meter Management
- System Administration

The second cloud use case is an implementation of a home healthcare scenario, i.e., of a system for monitoring, diagnosing and assisting people outside of a hospital setting. This example is a relevant area for TClouds because, for instance, Electronic Health Records (EHR) have recently shown a significant growth, as compared to the traditional "paper" versions. According to a report from marketing research firm Kalorama Information, until 2012, the market for EHR systems will grow by 14.1% annually. Main drivers of this trend are a growing need of hospitals to manage and exchange ever-increasing amounts of data and patients' demand for information and Internet-based opportunities for the self-management of health-related problems. As a global survey of hospitals and healthcare organizations[27] revealed, medical images, scanned documents, email and advances towards the EHR are going to be the cause for a meaningful increase in healthcare data, which is already a challenge for many hospitals.[28]

The broad setting is applicable to a multitude of important applications, e.g., remote monitoring of chronically ill patients, patient aftercare, assisted living for elderly, long-term monitoring, childcare, or health advice while travelling. We have decided to select innovative services for depressed patient's remote management as a concrete use case. This use case includes different actors and services:

- General Practitioner
- Patient
- Medical professional (e.g. Psychiatrist @ Hospital)
- Health and Wellness Service Provider (e.g. Activity monitoring service)
- Pharmacy
- Familiy
- Region/national authorities and infrastructure (e.g. Department of public health)
- TCloud of clouds:- Hosts PHR/EHR community cloud service(s) such as Microsoft HealthVault, or EPIC HER

While the short-term benefit of cloud computing in this setting is the increased connectivity and pervasive availability of health related services, a clear mid-term tendency is the need for more analytics, which require scalable computing power. As an example, statistical evaluation of long-term behaviour of bipolar patients can be used to detect early signs of depressions or manic episodes. Decision support systems can evaluate patient generated input (e.g., physical activity data monitored through a personal device), and help decide whether the patient should see a doctor or not. This requires computational power that can be provided by cloud computing in a scalable and cost-efficient way.

Healthcare operation is being migrated to ICT, and medical data is accessible interactively, transmitted remotely on a routine basis, and even copied for resilience reasons, e.g., backed-up. Protection of personal data and reliability of the output of the cloud are strong requirements and a substantial challenge. It will be demonstrated how sensitive personal data such as medical records can be protected in the cloud without reducing the offered resilience and availability, essential in particular in medical emergency situations.

The future cloud-enabled home healthcare services should support a wide range of applications. We aim to manage the complete life-cycle of a prescription through a web-based application hosted in the cloud. The patient can monitor his data, the general practitioner can provide prescriptions, and a pharmacy can retrieve and validate them. A particular feature that we plan to insert in this scenario is the possibility for the person to receive or reorder directly from home the needed drugs. Finally, once the drug has been delivered, the cost will be refunded though the regional health system.

In this case we plan to have a unique situation where an on-line application, based on cloud computing, is accessed by the different actors. Furthermore, the use of pervasive devices (drug cabinet, phone, or other appliances) makes this use case particularly suitable for a cloud deployment.

---

[27] BridgeHead, 2010. Report: The BridgeHead Software International 2010 Data Management Healthcheck Survey. Available online at: http://www.bridgeheadsoftware.com/pdfs/BH_Rpt_Data-management-survey-results_A4.pdf

[28] Nalin, M. & Baroni, I., 2010. e-Health Drivers and Barriers for Cloud Computing Adoption. Milano. To be published.

Cloud Computing has the potential to provide tremendous benefits for Healthcare Organizations. The BridgeHead survey indicated that the top priorities in the investments for IT budget in healthcare organizations in the near future are data backup, business continuity, and disaster recovery (priority for 44.3% of respondents), followed by PACS (Picture Archiving and Communication System; 37.7%), archiving (32,1%), server virtualization (31.1%), and storage virtualization (20,8%). Interestingly, only 15,5% of the respondents indicated Cloud Computing as an investment priority, while it could be an efficient solution for most of the aforementioned points.[29]

5 Exploitation Roadmap

The exploitation of the TClouds platform and TClouds assets and the implementation of these in other usage scenarios than the two examined and deployed in the TClouds project requires a coordinated action of all TClouds partners at an early stage of the project. It appears necessary that

- contacts to potential users and multipliers are established early, through the Advisory Board and the various contacts that are established through the research and workshops in Activity 1;
- insights in requirements and solutions are made visible early, in form of preliminary results;
- technical solutions are tested early in order to demonstrate the overall functionality of the platform and the applicability of the TClouds approach in the two selected usage scenarios;
- foundations are laid at the end of the project that interested users outside the TClouds consortium can easily and fast benefit from the TClouds platform and the TClouds assets.

To this end, the TClouds exploitation roadmap consists of three layers: requirements, context and impact analysis, R&D for the development of the equipment of the TClouds assets, and implementation and dissemination.

The detailed roadmap is illustrated in Figure 6. It shows that there is a constant and fast flow of information from all work packages towards implementation and dissemination. The aim is to have a defined set of companies, deriving from the advisory board and the ongoing dissemination activities at interviews, workshops and conferences, at the end of the project period that serve as early adopters, which, at the end, attract interest of ever more companies and multipliers.

Since the focus of the exploitation roadmap is on exploitation and not on the workflow between the different components of the project, relations between requirements, context and impact analysis and R&D for the development of the equipment are left out in Figure 6.

[29] Ibid.

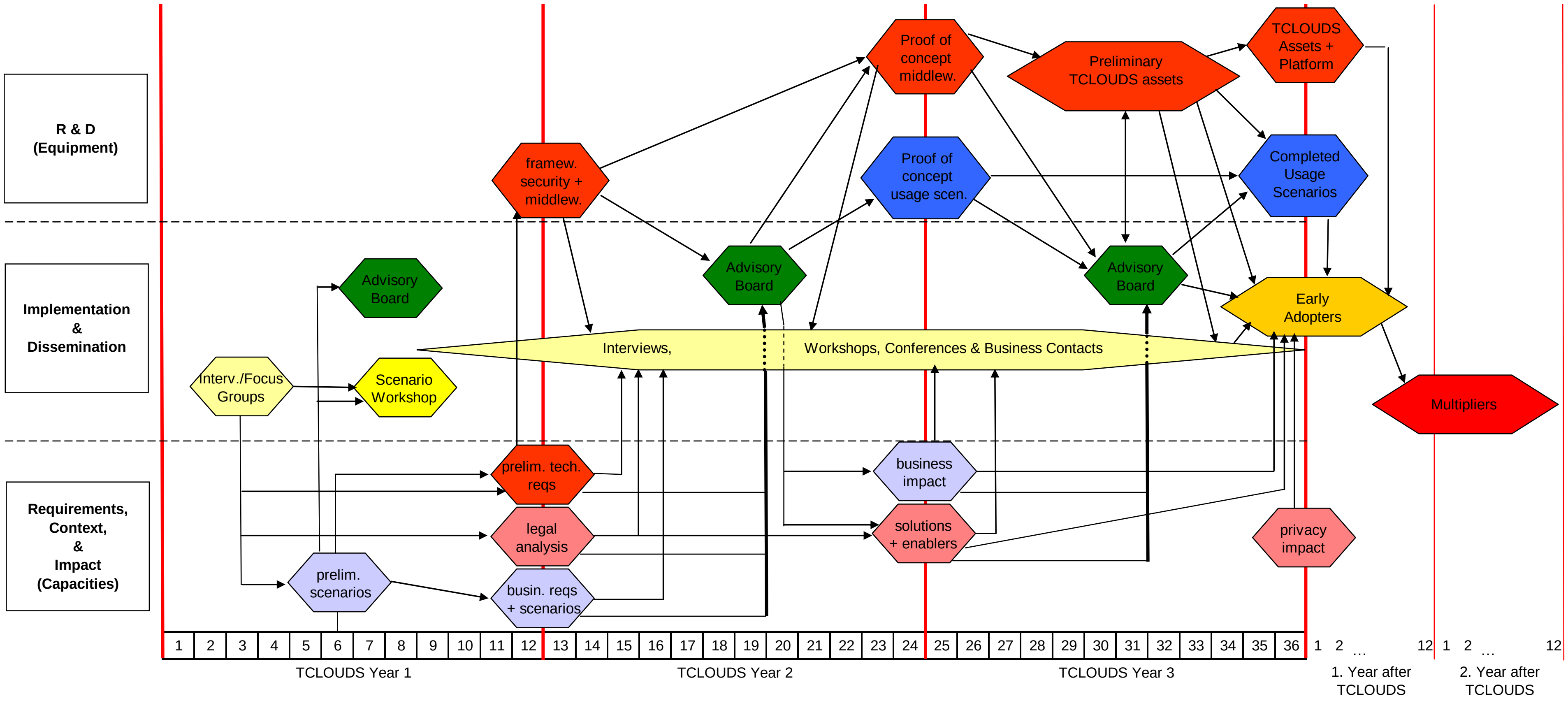

Figure 6: TClouds exploitation roadmap