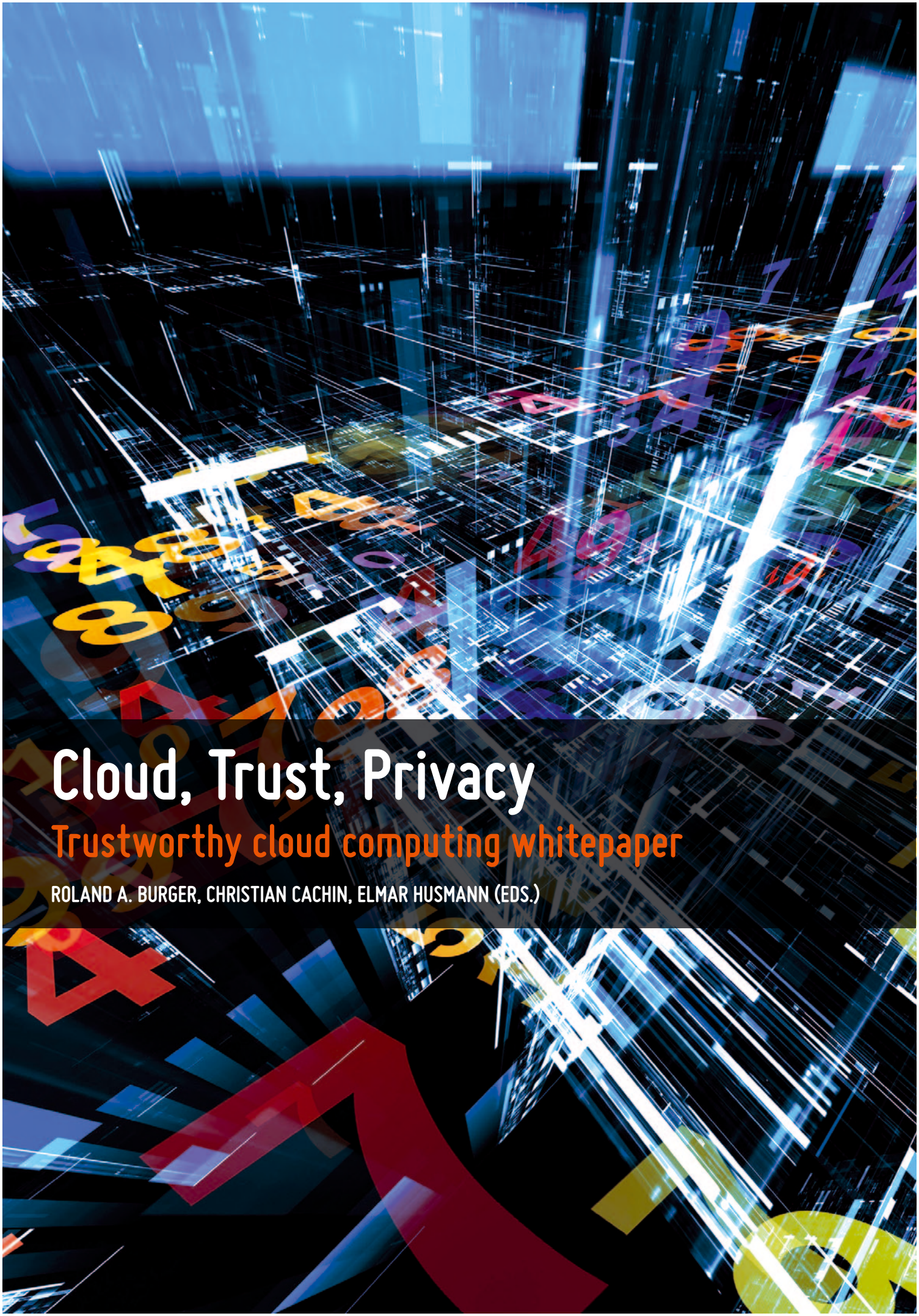


Cloud, Trust, Privacy

Trustworthy cloud computing whitepaper

ROLAND A. BURGER, CHRISTIAN CACHIN, ELMAR HUSMANN (EDS.)

















imprint

To get in touch with the Authors: r.burger@innova-eu.net or huselmar@de.ibm.com

Further information on the TClouds Project: http://www.tclouds-projects.eu

Graphical editing and production: Roland A. Burger & Elmar Husmann.
Pictures: TClouds, PhotoCase.com, Shutterstock, Thinkstock.

The TClouds project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT-257243.


Cloud, Trust, Privacy

Whitepaper 2013

TClouds

ROLAND A. BURGER, CHRISTIAN CACHIN, ELMAR HUSMANN (EDS.)

table of contents

Introduction

Existing cloud computing services today are generally not trusted for running critical infrastructure, which may range from business-critical tasks of large companies to mission-critical tasks for the society as a whole. The latter includes e.g. our complex service systems to provide water, electricity or health care.

TClouds (Trustworthy Cloud Computing for Critical Infrastructures) has been a research initiative funded by the European Union under the FP7 research program. This whitepaper presents key results from this project which has been the first large-scale EU research initiative entirely dedicated to privacy and trust issues in cloud computing. This whitepaper targets decision makers, analysts and cloud customers rather than computer science researchers. In the paper, we therefore provide an overview aimed at practitioners on both the problem as well as the solution space in trustworthy cloud computing.

This will be based on different results of TClouds – notably the outcomes of events and stakeholder consultations that we used to better understand the current market perception and "customer views" on privacy and security in cloud computing.

TClouds has proposed several security and privacy protecting enhancements to existing commodity clouds as well as an own resilient cloud middleware. Such areas of technical innovation are briefly described and linked to customer requirements. This is further investigated at case examples from the health care and smart energy domains.

Another cross cutting concern in TClouds has been the use of standards – in particular open standards – in a cloud infrastructure. In this paper we provide a mapping of security- and privacy-relevant standards in cloud computing that have been analyzed in depth in the project.

Finally, we provide an account of the debate that TClouds has started with European venture capitalists and entrepreneurs.

Chapter 1
Issues and Challenges in the current Cloud Market

STAKEHOLDERS

TClouds has conducted a stakeholder survey in two rounds in 2012 and 2013. Both rounds of the survey covered over 60 interdisciplinary stakeholders that have been polled with an online survey and phone interviews. Profiles of stakeholders included leaders from larger and small businesses, public sector organizations, venture capital and academia. Whereas the first round of the survey had investigated general business requirements and market issues towards cloud computing, the second round explored if TClouds technologies could motivate cloud users to adopt cloud computing in more privacy and security sensitive application areas. This chapter is based on results of the first survey round.

The survey has revealed clear benefits of cloud computing but also a profound range of concerns about the security and data privacy risks associated with state-of-the-art cloud services. Despite this, 78% percent of the TClouds stakeholders already use cloud computing to some extent.

Tangible Business

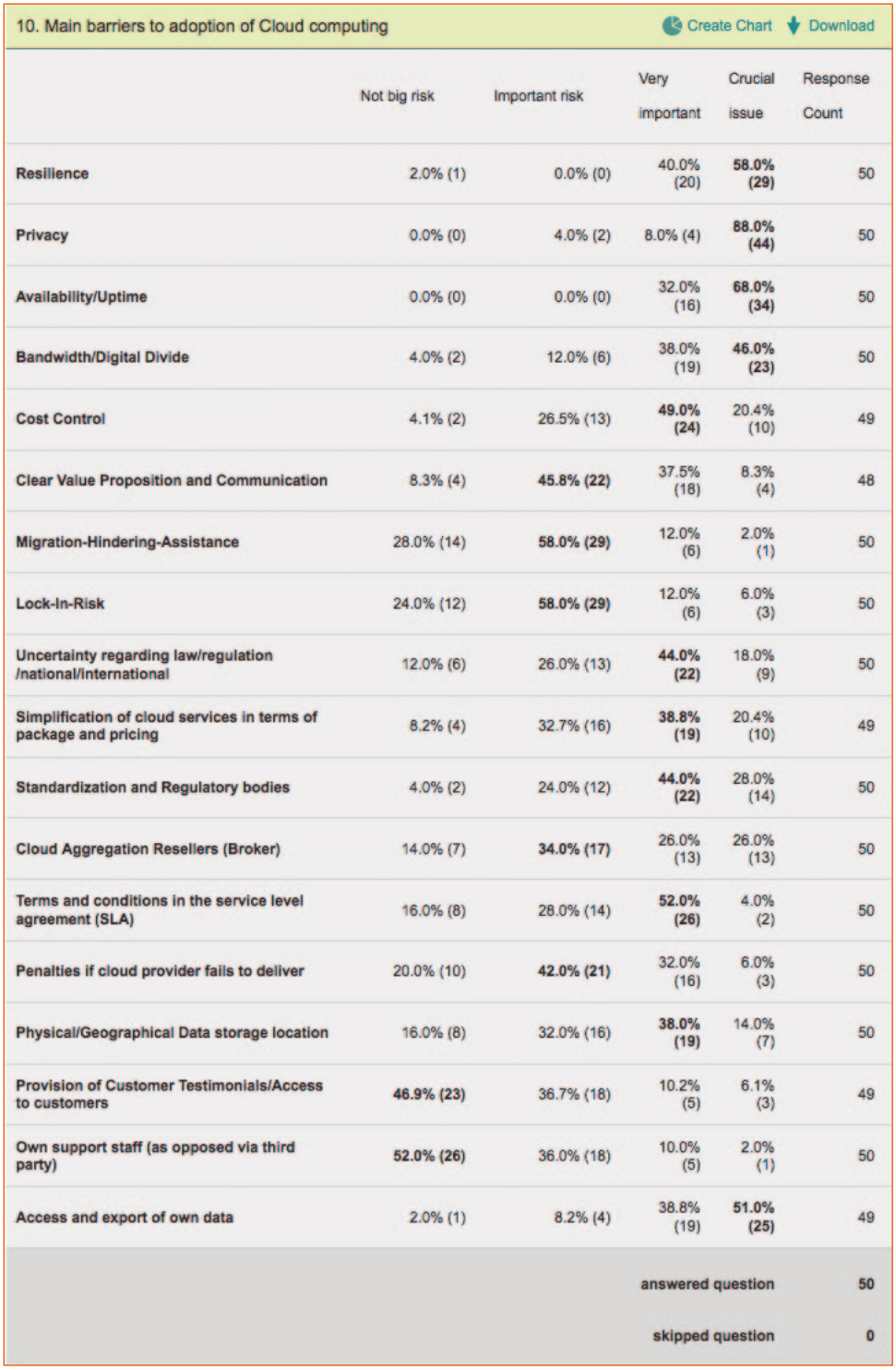
Figure 1 shows the results of a question on the reasons to adopt cloud computing. Clearly, financial reasons – e.g. the idea to reduce ICT investment costs and transfer them to service costs – top the lists of cloud computing benefits. Closely related to this are the objectives of scalability and business process acceleration. Hence, cloud computing is directly related for most stakeholders to tangible business benefits that can impact the bottom line.
These benefits appeal to different kinds of organizations. However, we could demonstrate a strong resonance from small to medium sized businesses (SMEs). For these organizations cloud computing would provide the opportunity to largely outsource ICT infrastructure management while remaining flexible and scalable in their dynamic business environment.

11. Why would you adopt Cloud (InterCloud) computing? Create Chart Download

	Not important	Important	Very important	Crucial	Response Count
Cost saving and Reduction (from CAPEX to OPEX)	2.0% (1)	2.0% (1)	12.0% (6)	**84.0% (42)**	50
Accelerate Business processes	2.0% (1)	2.0% (1)	10.2% (5)	**85.7% (42)**	49
Scalability (Easiness)	0.0% (0)	4.0% (2)	36.0% (18)	**60.0% (30)**	50
Green computing adoption	0.0% (0)	4.1% (2)	22.4% (11)	**73.5% (36)**	49
Reducing IT system heterogeneity	**50.0% (25)**	38.0% (19)	10.0% (5)	2.0% (1)	50
Lack of skilled IT personnel	**60.0% (30)**	32.0% (16)	8.0% (4)	0.0% (0)	50
Resilience of Business processes	12.2% (6)	**53.1% (26)**	28.6% (14)	6.1% (3)	49
Strong customer/business process consultation available	**52.0% (26)**	42.0% (21)	2.0% (1)	4.0% (2)	50
				answered question	**50**
				skipped question	**0**

Figure 1:
Reasons for adopting Cloud Computing

Figure 2:
Barriers to adopt cloud computing



10. Main barriers to adoption of Cloud computing — Create Chart — Download

	Not big risk	Important risk	Very important	Crucial issue	Response Count
Resilience	2.0% (1)	0.0% (0)	40.0% (20)	**58.0% (29)**	50
Privacy	0.0% (0)	4.0% (2)	8.0% (4)	**88.0% (44)**	50
Availability/Uptime	0.0% (0)	0.0% (0)	32.0% (16)	**68.0% (34)**	50
Bandwidth/Digital Divide	4.0% (2)	12.0% (6)	38.0% (19)	**46.0% (23)**	50
Cost Control	4.1% (2)	26.5% (13)	**49.0% (24)**	20.4% (10)	49
Clear Value Proposition and Communication	8.3% (4)	**45.8% (22)**	37.5% (18)	8.3% (4)	48
Migration-Hindering-Assistance	28.0% (14)	**58.0% (29)**	12.0% (6)	2.0% (1)	50
Lock-In-Risk	24.0% (12)	**58.0% (29)**	12.0% (6)	6.0% (3)	50
Uncertainty regarding law/regulation /national/international	12.0% (6)	26.0% (13)	**44.0% (22)**	18.0% (9)	50
Simplification of cloud services in terms of package and pricing	8.2% (4)	32.7% (16)	**38.8% (19)**	20.4% (10)	49
Standardization and Regulatory bodies	4.0% (2)	24.0% (12)	**44.0% (22)**	28.0% (14)	50
Cloud Aggregation Resellers (Broker)	14.0% (7)	**34.0% (17)**	26.0% (13)	26.0% (13)	50
Terms and conditions in the service level agreement (SLA)	16.0% (8)	28.0% (14)	**52.0% (26)**	4.0% (2)	50
Penalties if cloud provider fails to deliver	20.0% (10)	**42.0% (21)**	32.0% (16)	6.0% (3)	50
Physical/Geographical Data storage location	16.0% (8)	32.0% (16)	**38.0% (19)**	14.0% (7)	50
Provision of Customer Testimonials/Access to customers	**46.9% (23)**	36.7% (18)	10.2% (5)	6.1% (3)	49
Own support staff (as opposed via third party)	**52.0% (26)**	36.0% (18)	10.0% (5)	2.0% (1)	50
Access and export of own data	2.0% (1)	8.2% (4)	38.8% (19)	**51.0% (25)**	49
			answered question		50
			skipped question		0

Clear practical concerns

The strong support for cloud tangible benefits demonstrates one thing: cloud computing seems to be unlike many trends in the ICT domain where business benefits are unclear. But despite this clear perception of benefits, our stakeholders have revealed a long list of practical concerns towards cloud computing that are depicted in Figure 2. Among these reasons, privacy tops the list. Other key concerns relate to the availability as well as to the resilience of the cloud services.

An in-depth investigation was also made on three related issues: the openness of the cloud provider for auditing, for providing transparency on the implementation of the services as well as the general compliance with EU regulations – such as the EU data protection directives (see Figure 3).

A related concern was the geographical location of data storage and the related national jurisdictions that then apply and that differ from country to country. Overall the survey revealed that stakeholders are deeply concerned about details of the implementation of the cloud services and these strongly impact their decision for a specific provider.

Another area of concern is the risk of lock-in. This was cited by over 50% of respondents. Avoidance of lock-in risks is closely connected to the support of open standards by the cloud service and to the support of data access, export and migration. These have also been reported as important decision criteria for or against a cloud provider.

With regard to compliance, cloud providers need to provide evidence – while evidence could take different forms such as certificates or adherence to organization level standards (e.g. ISO family).

Skills gap

The development pace in the ICT industry is high and cloud computing is one of the latest trends. It implies not only a number of technical changes but – as importantly – significant changes on the side of the ICT organization. Notably, it implies changes in how ICT infrastructure is managed. While infrastructure had previously been considered an environment of physical resources owned by an organization (the inhouse data center) that needed technical administration and asset management, it is now becoming a more complex range of external cloud services. While need for technical administration and managing physical assets decreases, the need for service-, contract- and provider-management increases.

This shift results in the need for training and re-skilling personnel. And in fact, our stakeholders have widely cited this is one of their

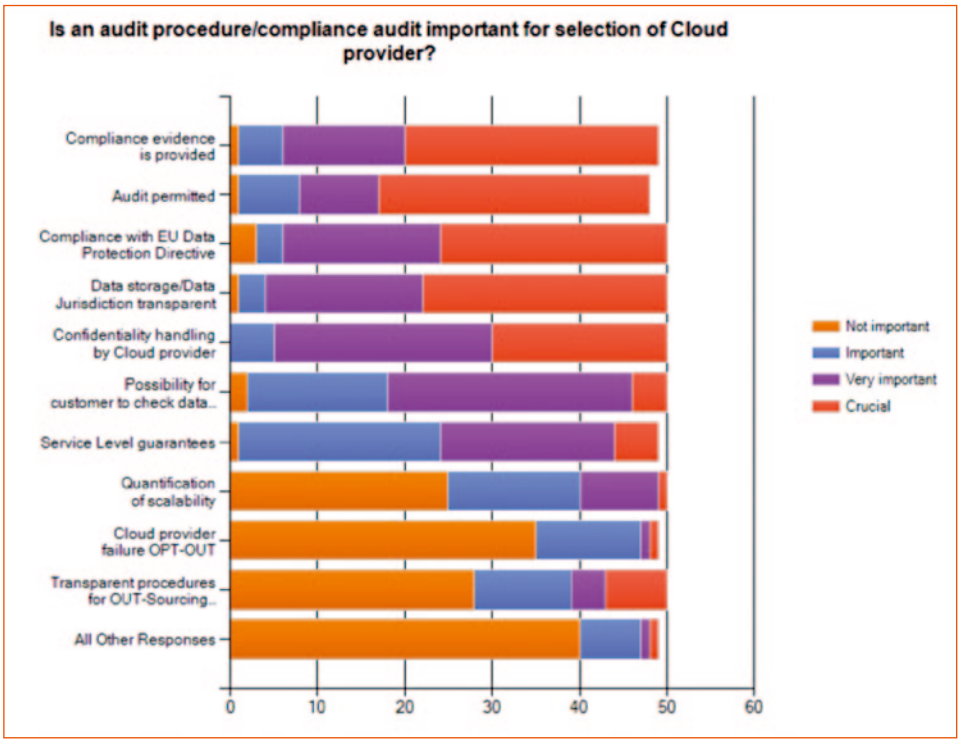


Figure 3:
Relevance of auditing, transparency and compliance

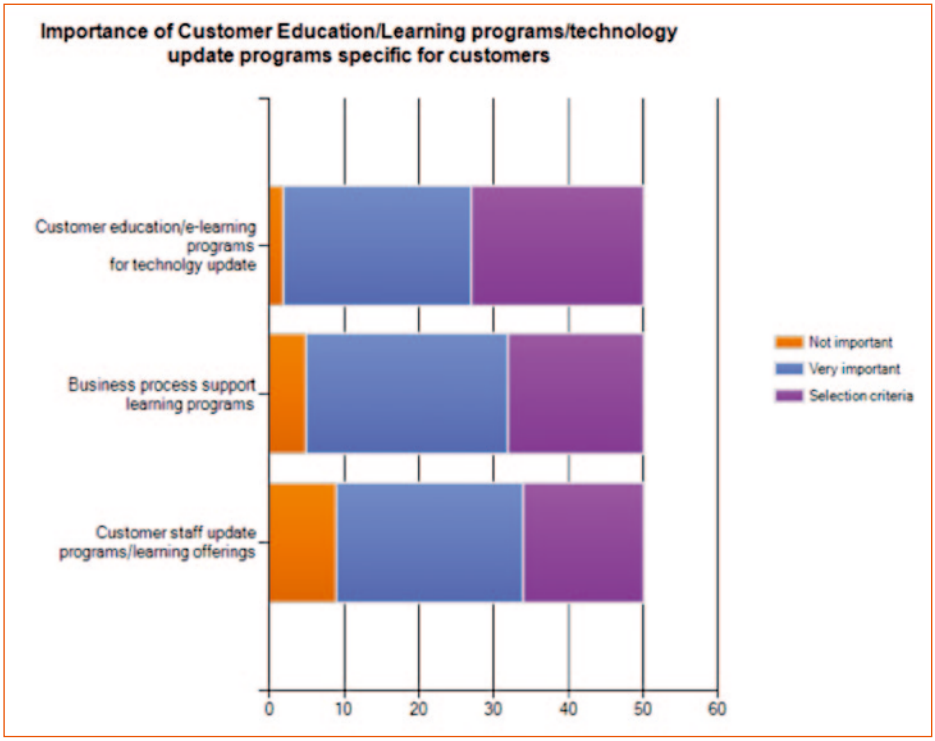


Figure 4:
Importance of training and re-skilling support

selection criteria for a cloud provider. In other words: adopting cloud computing is by no means a self-explanatory option and organizational implementation efforts should never be underestimated.

Training support is needed on the level of the cloud infrastructure technology as well as on the level of supporting specific business processes via application level cloud services.

Issues and Challenges

The first round of the TClouds stakeholder survey and interview series has shown that the current market reception of cloud computing is polarized between clear perceived benefits on the one hand and a large number of practical concerns on the other hand – with privacy and trust playing a key role. While we will investigate these trust and privacy concerns in more detail in this paper, the benefits of cloud computing that were widely supported by our stakeholders can be summarized as follows. We have also been able to show that this applies to different types and sizes of organization – while in particular small to medium sized companies (SMEs) reported to benefit from scalability, ramp-up time reducation and flexibility of cloud computing.

- **Reduced Capex & Opex costs** – cloud computing offers cost advantages in terms of reduced costs, both in terms of initial outlay investments (Capex) and ongoing operational costs (Opex) such as IT resource & power/energy.
- **Performance, durability & high availability** – cloud computing offers high performance and scalability right from the start. This can in particular be important for launching new businesses or services.
- **Scalable storage** – storage needs can seamlessly increase rather than expensive hardware acquisition.
- **Always up to date** – In addition an important aspect is the missing need to worry about future updates, patch levels etc. for software and hardware.
- **Remote access from multiple devices** – The trend to a mobile workforce is clearly a growing issue. Many organizations need to provide access to information and company services on the go and an on increasing range of devices – including those of their employees (bring your own device).
- **On-demand** – The simple scaling of computing resources has a huge attraction in particular for organizations in dynamic business environments with growing or seasonal workloads, that can easily be satisfied by turning up bandwidth and/or processing power.
- **Energy and operation cost efficiency** – cloud computing uses massively pooled hardware resources and can be designed to consume less energy than traditional in-house data centers.
- **Ramp-up advantage** – Without the need for implementation of hardware and various other components, ramping up times can be dramatically decreased – e.g. for new Internet based services
- **Specifically skilled workforce** at large cloud provider companies that can better and more effectively cope with exceptional situations such as downtimes, cyber attacks etc.

Figure 5:
Summary of
cloud market benefits

Chapter 2
Cloud Security and Privacy

With the clear support of cloud business benefits from the first round of our stakeholder survey, as well as the counter-balancing expression of concerns, TClouds conducted a second round of the survey and interviews to investigate the areas of cloud security and privacy concerns in greater detail.

THE PROBLEM AREAS*

The following more specific security risks raised high concerns among the stakeholders (% indicates sum of replies as "relevant" or "highly relevant"):

1. Cloud specific attacks by externals (88%)
2. Accidential leakage of data and credentials (82%)
3. Insider attacks (e.g. by cloud administrators) (82%)
4. Insufficient protection against more general IT security risks and attacks (75%)

Also, the TClouds stakeholder expressed concerns about the dependencies when working with a single cloud provider. Most relevant concerns in that context were:

1. Breach of confidentitality (85%)
2. Interruption of the service (85%)
3. Impossibility to restore data or computation after a disruption (85%)
4. Loss of data (78%)

While third party auditing and security policies defined by the provider where reported to be important, the TClouds stakeholders attributed great importance to user control as well. Least importance was attributed to monitoring mechanisms that are entirely in the hand of the cloud provider.

The preferences were as follows:

1. Full user control of security policies (70%)
2. Third party auditing, monitoring and certification (68%)
3. Mechanisms in place to self monitor security state (65%)
4. Security policy options pre defined by the cloud provider (65%)
5. Provider takes over security monitoring (52%)

In terms of the overall requirements on trustworthy cloud services – the following factors were seen as important:

1. Data portability support (98%) – with 63% as "highly relevant"
2. Support of open standards (75%)
3. Support of de-facto standards (e.g. Amazon APIs) (73%)
4. Availability of components as open source (58%)

In particular, the TClouds stakeholders have given a strong statement for the need for openness, standards and data portability.

** Possible judgements were:*
not relevant,
somewhat relevant,
relevant,
highly relevant.

MARKET DEBATE

In the two rounds of the survey as well as in the supporting stakeholder events, a number of cross cutting themes emerged and were debated. We are not able to provide simple answers to these. Mostly, we expect that they will further determine the cloud debate in the upcoming years.

Overall, it emerged from our stakeholder consultation that there is a space in the market – and still development potential – for differentiated privacy-enhancing cloud services. This could also further open up the cloud market to sensitive application domains that would currently not be considered for using cloud services.

- **Price vs. privacy**
  While the importance of privacy has been widely supported, our stakeholder community has also supported that cloud computing is closely linked to business cost reduction cases. Therefore there is always a tradeoff between the privacy and security level that can be provided and the acceptable costs.

- **Differentiated levels of cloud security**
  In particular, stakeholders are supporting the need for differentiated cloud services that offer different levels of security and privacy protection. In this context, there was a strong support for the kind of high security infrastructure clouds that could be built with TClouds technologies, for intended deployment in high-end secure cloud services.

- **Support for privacy- and security- enhancing services**
  While the cloud provider might offer differentiated services, there is a further strong support for specific add-on products and security services that offer specific solutions for cloud security and privacy problems.

- **User control vs. comfort**
  While user control of cloud security and privacy has received strong support, there was also an expression of the need for comfort. This support for comfort can be achieved by creating packaged solutions as well as guarantees on the side of the cloud provider.

- **Open standards vs. de facto standards**
  While it was supported by the stakeholders that cloud providers have to support de facto standards such as the Amazon EC2 and S3 APIs, there was also a surprisingly strong support for open standards. This runs despite the fact that currently in cloud computing open standards are much less pervasive in commercial solutions.

- **Some concerns about the use of Trusted Computing hardware**

While some of the TClouds technical innovations use Trusted Computing hardware (see next chapter) and have received general support and interest by stakeholders, there were also considerable concerns expressed regarding the dependency on such hardware. This relates to issues of openness, the creation of single points of failure as well as cost implications.

- **Need for more for open-source cloud components**
  While not being as highly supported as open standards in cloud computing, it was also supported by the stakeholders that key TClouds technical components to enhance privacy and security should be available as open source. In particular, the enhancement of the Open Stack cloud platform was positively commented in this context.

Chapter 3
Building blocks for a trustworthy cloud infrastructure

The TClouds project has done intensive technical research and development work to pilot new approaches for making cloud computing more privacy protecting and secure. It would go beyond the scope of this paper to explain each area in technical depth. The TClouds technology innovation leaflets can be consulted for more detail.

The following also shows that TClouds research results have already taken their first steps towards productization and impacting market leading Open Source cloud frameworks like Open Stack.

For the sake of discussing with our stakeholders community, we have subdivided the TClouds technical innovations into 4 areas that can be regarded as building blocks for trustworthy infrastructure clouds.

AREA 1:
Trusted Infrastructure Cloud

What it is about:
TClouds has developed a solution based on trusted computing (TC) hardware to provide a high-secure infrastructure cloud. In particular, this cloud can ensure full verifiable integrity of resource allocation (e.g. where data is stored or computation takes places in the cloud) and is immune against insider attacks or other attempts to compromise these resources.

While putting demands on specific hardware installations in the cloud data center, the TClouds trusted infrastructure cloud provides a view into high-end possibilities for ensuring cloud trustworthiness.

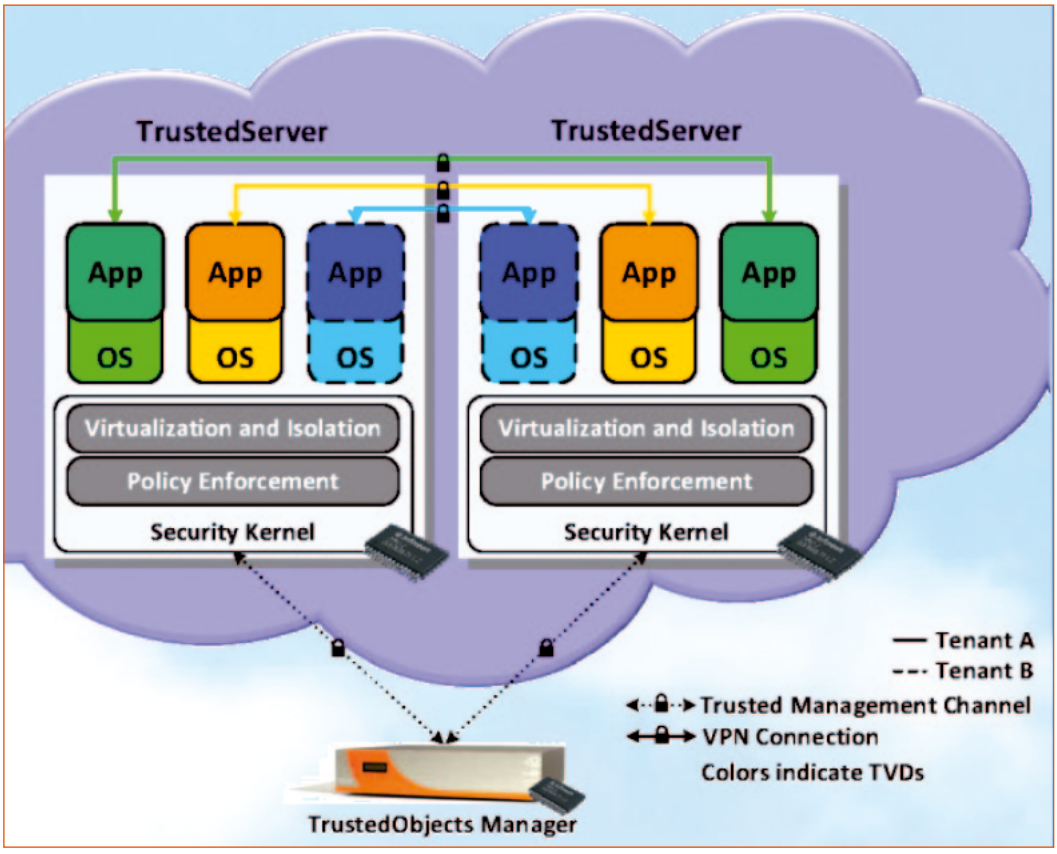


Figure 6:
Trusted Infrastructure Cloud derived from TClouds Research, showing three Trusted Virtual Domains in different colors

Reactions:
There was a strong interest by stakeholders in such a trusted infrastructure cloud. Most relevant application domains in that context were seen as:

1) Business Critical Workloads (83%)
2) Privacy sensitive data or computation (71%)
3) Critical Infrastructure (68%)
4) Location sensitive data or computation (67%)

Only a much smaller group saw a need for using trusted infrastructure clouds more general for all workloads (43%). So the stakeholders expressed that a trusted infrastructure cloud would at best be reserved for specific critical application cases.

In this innovation area almost equal support was expressed for the exploitation routes of a specific family of software & hardware products (58%), a premium trusted cloud service (58%) and general upgrading of clouds with TC elements (57%).

At the same time, vendor lock-in risks (85%), openness and flexibility concerns (77%), added management complexity (75%) and price (73%) where seen as roadblocking factors for the use of trusted computing technologies in cloud computing

AREA 2:
Trustworthy Open Stack

What it is about:
The second investigated area were security-hardening mechanisms for standard cloud platform software. In particular, TClouds has investigated the popular Open Stack cloud platform from a security perspective. This has revealed a number of security weaknesses and potentials for attackers to intrude cloud services build on Open Stack.

Areas of concern were e.g. the handling of cryptographic credentials in an Open Stack cloud or the verification of isolation and security policy enforcement. Figure 7 gives a brief overview about these enhancements.

Reactions:
TClouds stakeholders very strongly supported this area (88% overall) as relevant (40%) or even highly relevant (48%). With most seeing this as an integral part of all cloud platforms of the future. At the same time, TClouds stakeholders saw an emerging market of specific cloud platforms for high security solutions (78%) and add-on cloud security tools and services (75%).

Figure 7:
TClouds — Enhancements to Open Stack

	TClouds Enhancements to Open Stack
Access Control as a service	Trustworthy Cloud Scheduler. Matching User security & privacy requirements to cloud virtual resource allocation. Cloud security policy enforcement.
Cryptography as a service	Protection and user empowerment while deploying high value cryptographic credentials to the cloud.
Security Assurance in Virtualized Environments	Verify isolation among different tenants in platform
Remote Attestation Service	Assess the integrity of nodes in the Cloud infrastructure.
Secure Log Service	Support different secure logging schemes. Guarantee the log integrity and authenticity in monitoring the cloud.
Ontology based reasoner	Management of trusted virtual domains in the cloud

For more information, please refer to the TClouds technical factsheets: http://www.tclouds-project.eu/index.php/home/factsheets

AREA 3:
Mechanisms to self-monitor & screen Cloud Security State by the User

What it is about:
The third investigated area were mechanisms and tools to self-monitor and screen cloud security state by the user. TClouds has developed several methods to scan the virtual topology of clouds as well as investigate security state from the user side.

Reactions:
This also received a strong support of 65% of the TClouds stakeholders. The same holds also for Mechanisms to express and control Cloud Security Policies by the User. This received an even slightly higher support of 70%.

AREA 4:
A highly resilient Cloud Service built on a Cloud of Clouds

What it is about:
TClouds researchers have developed technologies to use multiple clouds at the same time to distribute stored data and for running services. This increases resilience over using a single cloud. For storage, this uses space efficient data replication and a key value store (KVS) interface provided by most cloud providers today. A key-value store (KVS) offers functions for storing and retrieving values associated with unique keys. KVSs have become widely used as shared storage solutions for Internet-scale distributed applications. So it demands no specific adaptations on the side of the provider.

The cloud-of-clouds approach tolerates service outages and security incidents affecting individual clouds. Although existing cloud platforms provide high availability and reliability using internal replication, some common failure modes remain and services in the intercloud tolerate those.

Reactions:
68% of TClouds stakeholder expressed support for this. However, potential cost increase (85%) and performance restrictions (73%) were regarded as roadblocks to this technology.

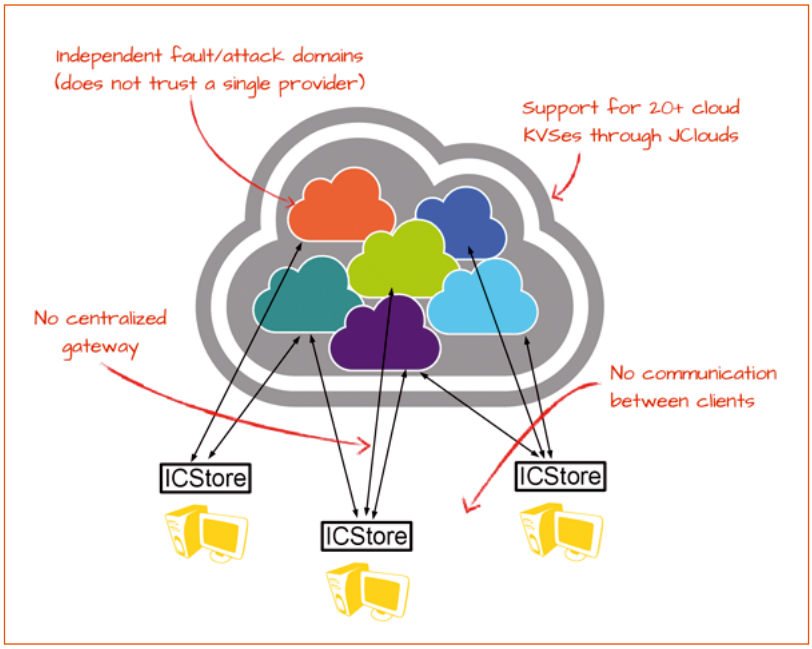


Figure 8:
A cloud-of-clouds storage system for key-value stores (KVSes)

Chapter 4
A Foundation for critical cloud applications

TClouds has investigated two different application areas, in order to better understand customer requirements towards cloud services: health care (with the San Raffaele Hospital, Italy, and Philips Healthcare) and smart energy (with Electricidade de Portugal and EFACEC).

Cloud providers usually adopt a one size fits all approach. The size of the health care market is massive and thus offers a great opportunity for a specialized cloud computing service offering, meeting the specific needs of all healthcare stakeholders. Tailoring of cloud services is needed to better meet the needs of users from a specific domain.

FOUR EXAMPLES
of requirements towards cloud providers for health care applications:

1) **Mandatory Security Breach Notification – Secure Logs:** TClouds has implemented secure non-modifiable logs at cloud infrastructure level, a log that records all access, authorized or unauthorized, at a granular level. Similar log technology has to be used at platform level, so that any breach could be notified to all users. In many current systems, log entry creation is still subject to misuse as it relies on the transparency of the platform governing system and staff.

2) **Conformity with HIPAA (health insurance portability and accountability act) standards on medical data location and transfer.** This popular standard in the US healthcare system specifies in detail the treatment of electronic medical records and patient data and the prevention of fraud and abuse. One element is the granting of permissions by the data owner – e.g. for data copy to different locations – as well as the logging of all such activities. In particular, standard cloud providers are not used to provide accountancy of data location as well as full transaction logging. TClouds demonstrates with the trusted infrastructure cloud and the secure log service that both is however implementable to infrastructure clouds in a way that would make them compliant to the high demands of health applications.

3) **Encryption of data in transit and storage.** For hospitals and health systems to ensure an appropriate level of security they could leverage the supplied TClouds Platform libraries of security protocols. Application developers will be forced to ensure appropriate encryption of data during storage, transit and processing. i.e. Decryption should only be necessary when visualizing the data and results.

4) **Granular data control.** With the increasing protection of patient information, there are concerns in the academic community about being deprived of data that is critical for medical research. Teaching hospitals, such as TClouds partner Hospital San Raffaele Italy, that have mandates for teaching and

research while operating as a hospital, need to give physicians access to appropriate case studies and records whilst researchers also need to have access. Security is needed, but the huge body of data should still be accessible in some way for research and moving the medical science forward. TClouds has demonstrated that granular data control is possible to share only the data elements relevant e.g. to a research study. A secure log service would also document all use and access to data.

Requirements in a smart energy grid application

Whereas in the healthcare domain the clear focus is on protecting the privacy of medical records and other patient data, in the smart energy domain, the focus has been stronger on protection against cyber attacks.

TClouds has investigated – with its partner EDP (Energias de Portugal) the linkage of cloud services to a critical physical infrastructure including a direct link to the SCADA (supervisory control and data acquisition) environment that controls street lighting units in major Portuguese cities (Figure 9).

It is obvious that such infrastructures provides for multiple interests to be attacked and notably cloud providers need to prevent that the interfaces they have to such control services can not be exploited in non-authorized ways.

The functionalities realized in the TClouds Smart Lighting example allow power grid operators to act upon public lighting with more information, ensuring the most efficient control. Also, municipalities are able to directly monitor the system, which allows them to make more specific and strategic decisions.

The Smart Lighting system is based on a cloud environment, which brings to the utility the scalability and computational power needed to manage a system with this level of geographic expansion and constant integration of new assets. Smart Grid components in general and public lighting in particular involve many different kinds of technical devices which, in many cases, are vulnerable to failures or damage. With a cloud based solution using TClouds' security components this impact is reduced, bringing a higher reliability to the system.

From the utility point of view, cloud computing adds flexibility to hardware investment plans. It allows lower starting investments and also the possibility to evolve the solution to follow changing requirements.

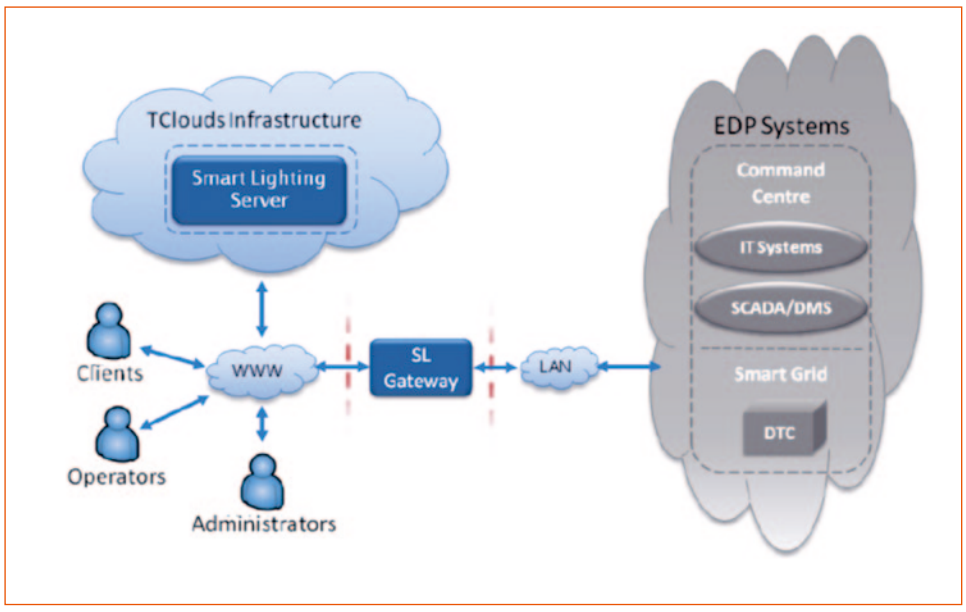


Figure 9:
Cloud service connected to smart grid control

Cloud, Trust, Privacy

Trustworthy cloud computing whitepaper

Chapter 5
Open standards for trustworthy clouds

The Clouds project has done a careful investigation of the role of standards and in particular open standards for trustworthy cloud computing. The need for open standards in cloud computing was also supported by the TClouds stakeholders (Figure 10).

How important are the following criteria for you when selecting cloud services or products? [Support of open standards]

Answer	Count	Percentage
not relevant (A1)	1	1.67%
somewhat relevant (A4)	14	23.33%
relevant (A2)	18	30.00%
highly relevant (A3)	27	45.00%
No answer	0	0.00%

Standards in cloud computing however are a complex subject. In fact, cloud infrastructures are complex and relate to multiple levels of technology and ICT organization. Standards can occur on all levels and they may all have specific implications on security and privacy. For this reason, TClouds has distinguished several levels by their role in a cloud infrastructure and provided a map of relevant standards on all these levels.

Researchers in the TClouds project have subsequently investigated all these standards in more detail and analyzed them for current support or missing elements for trustworthy cloud computing.

In particular, we are distinguishing the following levels:

- **Organisation Level:** Standards concerned with management processes and organisation level security. This addresses first of all the providers of cloud services and the related operational processes in cloud data centres. It may also relate to the corresponding management processes of the user.
- **Semantic Level:** Standards concerned with the definition of entities, roles, terms and logical relations in infrastructure cloud computing – thereby supporting a semantic matching of organisation level requirements to the entities in the infrastructure.
- **Service & Application Level:** Standards concerned with the description, orchestration and deployment of applications, processes and services that build on top of infrastructure clouds.
- **Infrastructure Topology & Validation Level:** Standards concerned with the topology description of the cloud infrastructure and of the security goals as matching directly to the infrastructure. On this level, we are distinguishing between the description of the "desired" topology, the description of security goals (e.g. isolation) and the description of the "actual" live topology at it is encountered in the cloud.

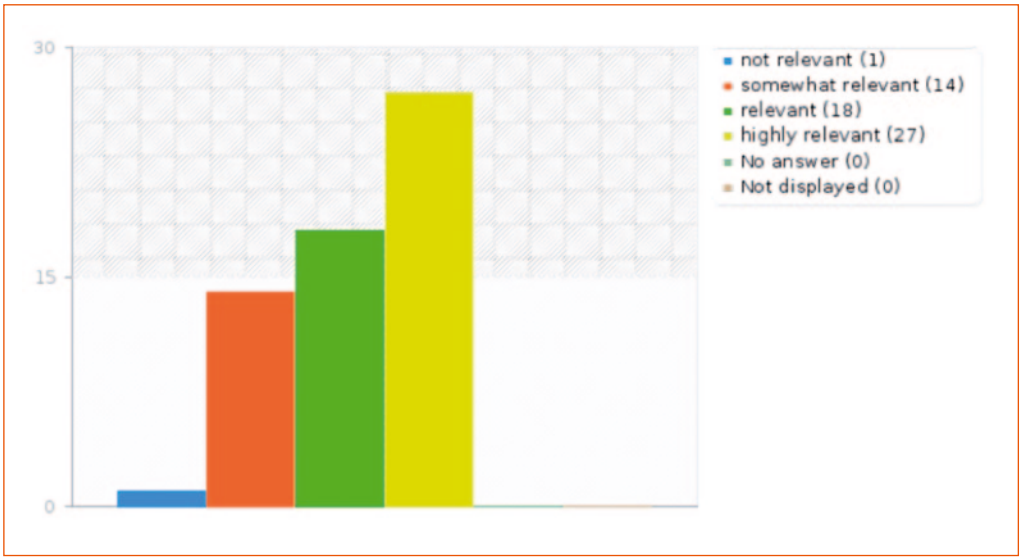
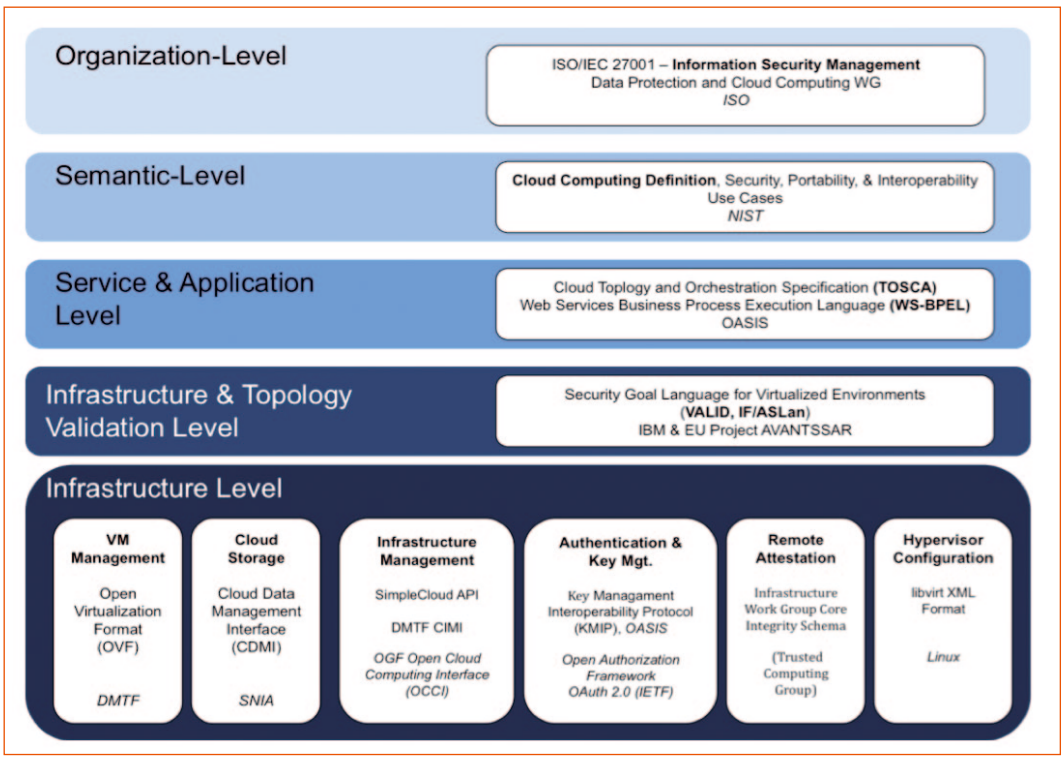


Figure 10:
Support for open standards in cloud computing among TClouds stakeholders

- **Infrastructure Level:** Standards concerned with the technical operation of the infrastructure such as interfaces specifications or data formats. We are distinguishing in our map the following sub-areas at the infrastructure level:
  - **Infrastructure Management:** Interface standards relating to the management of the infrastructure. This includes the triggering of actions by the infrastructure (such as the deployment or migration of a VM). It also includes the access to security relevant live information from the infrastructure.
  - **VM Management:** Data standards for virtual machine images as well as meta data standards relating to the deployment and execution of the VM.
  - **Hypervisor Configuration:** This concerns the direct configuration of the virtualization software used.
  - **Cloud Storage:** Data standards for data storage in the cloud as well as related meta-data standards (e.g. for the lifecycle of data in the cloud or the type and object structure of data).
  - **Authentication:** Authentication standards are concerned with the management of secure user credentials to access the cloud and its services. Related authorization standards are concerned with the description of the access level of a user – e.g. authorized activities, access to specific secure domains etc.
  - **Key Management:** Key Management standards are concerned with the handling of encryption keys to access encrypted data or process encrypted VMIs in the cloud. Also both, the Authentication & Key Management areas, provide a link into enterprise wide infrastructures for authentication and key management.
  - **Remote Attestation:** Standards concerned with the integrity verification of components of the cloud infrastructure and the attestation of this.

A number of other standards will apply in a secure cloud scenario including e.g. standards for secure data transmission (such as HTTPS). However these are relatively unspecific for the domain of cloud computing and we have not assumed a need to adapt them to the specifics of cloud. Hence they have not been included in the map.

Figure 11: TClouds Map of Open Standards



Sharing the TClouds map and analysis of standards

Standardization is a multi year process that demands a significant investment of time and efforts. However TClouds has achieved to interact with relevant bodies. This has included:

- The European SIENA and CIRRUS initiatives on cloud standardization (that included organizations such as NIST, OMG, DMTF, OGF, OASIS and SNIA)
- CEN/CENELEC
- DIN and ISO/IETF
- W3C

A central aim of this interaction has been to highlight the TClouds map of standards and specific related issues for trustworthy cloud computing.

TClouds has also interacted with European private organizations such as the Cloud Security Alliance.

Much of the debate around cloud standards is at an early state – in particular when it comes to more attention to secure cloud computing. So a next concrete step in which TClouds is involved is the creation of a related CEN Workshop agreement. The mapping analysis done in the TClouds project therefore provides a good support of crystallizing out the interplay of different security relevant elements and complementary standards in cloud computing.

This also goes along with the fact that the standards named in the TClouds map are only partially implemented yet in commercial cloud services and products. So, standardisation in clouds will still demand significant research and commercial engagements in the upcoming years – and we are just standing at the beginning.

W3C Tracking Protection (DNT standard)

TClouds members IBM and ULD have been closely involved in the W3C Tracking Protection Workinggroup. A first standard that has been issued by the group is the Tracking Preference Expression (DNT) that already has been adopted – e.g. by the Mozilla Foundation for the Firefox Web Browser.
Still debates are ongoing with providers to adopt DNT and customize services accordingly.

The DNT standard provides a first interesting step towards the automated expression of preferences from the side of Internet service users (mostly end users and consumers) towards cloud providers.

DIN and ISO/IETF

TClouds partner ULD further has been closely involved with several stakeholders and members of the German DIN institute to discuss and contribute to several ISO/IETF standard drafts such as the draft 27018 “Code of practice for data protection controls for public cloud computing services” and draft 29102 “Privacy Architecture Framework”.

Chapter 6
A discussion with venture capitalists and entrepreneurs

Cloud computing is a dynamic market field. It is determined by large players – such as Amazon and Google – but also research and entrepreneurial activity. TClouds has organized in 2013 several events to further discuss – in addition to the stakeholder survey and interviews – TClouds research results and innovations outside of a pure research community.

The events included a cloud privacy and trust panel organized at the Conference for Computers, Privacy and Data Protection 2013 (CPDP), a workshop at Oxford University (consistent of a technical event and a TClouds presentation at the Oxford Entrepreneurs MeetUp) as well as a workshop at Cambridge University (including the participation of the Cambridge Idea Accelerator, the Spring Board StartUp Incubator and the Venture Capital Firm Amadeus Capital Partners represented by its founder Hermann Hauser).

The TClouds events in Oxford and Cambridge offered the possibility to discuss in detail with the entrepreneurial community of one of Europe's and globally leading high tech cluster regions. This included discussions with students, start-up entrepreneurs as well as serial entrepreneur and venture capitalist Hermann Hauser, who has a personal track record of creating highly successful companies in the IT world, including ARM processors and Acorn computers.

This debate is unusual for European ICT research projects and turned out to be inspiring for both sides. A general hot issue in the debate was for what application areas cloud computing would be acceptable, how this will develop in future and how the application domains of cloud computing could be further extended with the help of TClouds technologies. In that context, Mr. Hauser and others pointed to the observation that the cloud market seems to diverge into a highly cost sensitive mass market (with many services either for free or at strikingly low costs) and a high-end market with a wider range of user control, security and privacy protection. It was also debated that the price differences between services on both ends can be significant and are often not directly reflected in the differences of hardware, software and operations costs. So mostly they reflect a different type of business model.

Mr. Hauser pointed out that he generally believes in the prospects of bringing more security and privacy protection to mass cloud services. This could be presented to consumers as alternative services in a similar form as mobile apps existing in "for free" (e.g. cross financed by advertising) and "for cost" versions with acceptable – limited – add on costs.

Figure 13: TClouds informal presentation at weekly meeting of the Oxford Entrepreneurship society

Figure 14: TClouds Cambridge Venture round Moment of discussion with VC Hermann Hauser and entrepreneurs

Figure 15: TClouds workshop Oxford: Jonathan Sage – IBM Cloud Policy Leader EMEA

Conclusion
& Outlook

This whitepaper has shown that security and privacy in cloud computing are key concerns from the viewpoint of a diverse group of stakeholders – including notably many cloud customers and decision makers.

While many of the security and privacy concerns are crosscutting, there are also specific demands of application domains like healthcare that currently are reluctant to adopt cloud computing. In this paper we have therefore investigated the broad "security & privacy" concerns towards cloud computing in more detail and sub divided them into a number of practical questions such as guaranteeing integrity of the resources, of data locations, encrypting data in storage or transit, the prevention from insider attacks or finding non-modifiable ways of logging activities.

We have already demonstrated that the enhancements and technical innovations developed by TClouds may effectively address such concerns. This would indeed open up the potentials of cloud computing to be used in more sensitive application domains – like business critical data or critical public infrastructure.

As a research project, many of the TClouds innovations are of course in a demonstration stage and just gradually being productized.

However first commercial successes have grown out of TClouds. They include the SAVE technology for security analysis of virtual systems commercialized by IBM and the enhanced Trusted Management Components and Trusted Cloud Nodes in the Trusted Infrastructure by Sirrix. Moreover, open-source toolkits like DepSky are being adopted by academic and commercial users.

In the same way, as cloud "security & privacy" sub divides into a broad range of more detailed requirements and concerns, TClouds technical innovations can be seen on the one hand as point solutions for specific problems but on the other hand can also be seen as a toolkit and architectural approach to security-harden cloud infrastructures overall.

In fact, security-hardening clouds demands an architectural approach and changes at multiple levels. In the same way, the use of standards in cloud computing needs to be well thought through – and rather demands a proper mapping than a decision for only one or two key standards.

TClouds has investigated these different levels and elements in detail. We expect to see in the future on the one hand interesting point solutions for cloud security and privacy problems as well as more holistic cloud services that offer different levels and packages for security and privacy. The workshops done so far and the interest received, make us confident, that the work of TClouds will continue to bear fruits.

Cloud computing is becoming one of the central paradigms of computing at the beginning of the 21st Century. The large scale European research initiative TClouds has investigated cloud security, trust and privacy at the intersection of cutting edge research, market-, legal- and business analysis, technology transfer and interaction with European entrepreneurs. TClouds brings together 14 partners from 7 different countries that are at the forefront of these developments.

WWW.TCLOUDS-PROJECT.EU