Publishable Summary

Project number:	257243
Project acronym:	**TClouds**
Project title:	**Trustworthy Clouds** - Privacy and Resilience for Internet-scale Critical Infrastructure
Start date of the project:	01.10.2010
Duration:	36 months
Programme:	FP7 ICT IP

Date of the reference Annex I:	10.12.2012
Periodic report:	Publishable Summary (as part of D4.2.2 "2nd Periodic Report according to EC regulations of the model contract")
Period covered:	01.10.2011-30.09.2012 (M13-M24)
Activities contributing:	All
Due date:	30.09.2012 (M24)
Actual submission date:	24.05.2013 (D4.2.2 Version 3.0)

Project Coordinator:	Technikon Forschungsgesellschaft mbH (TEC)
Tel.:	+43 4242 233 55
Fax:	+43 4242 233 55 77
E-mail:	coordination@tclouds-project.eu
Project website:	www.tclouds-project.eu

2 Publishable Summary

Project name: **TClouds** *Start date*: 1st October 2010
Grant Agreement: **257243** *Duration***:** 36 months
Project website: http://www.tclouds-project.eu/
Contact: coordination@TClouds-project.eu

Mission of TClouds: *To develop an advanced cloud infrastructure delivering computing, networking, and storage that achieves a new level of security, privacy, and resilience yet is cost-efficient, simple, and scalable. To change the perceptions of cloud computing by demonstrating the prototype infrastructure in socially significant application areas: energy and healthcare.*

The TClouds Project: TClouds envisions and builds a Future Internet where federations of standardized resilient and privacy-protecting global infrastructure clouds offer virtualized computing, communication, and storage resources that allows hosting of critical and non-critical ICT systems. Particular focus is placed on privacy protection in cross-border infrastructures and on ensuring resilience against failures and attacks.

Motivation: State-of-the-art cloud computing enables seamless access to services and global availability of information, but inherent risks severely limit the application of this technology. In a cloud environment, pertinent data is accessed via information and communications technology (ICT) using remote hardware instead of being stored only on a local server or computer. The benefits of increased storage at reduced cost allow information to be made readily available. However, the current cloud computing model comes with perceived risks concerning resilience and privacy. There are three fundamental trends in ICT whose risks mutually reinforce each other:

- the push towards an Internet of Services - most services are provided on the web as a platform;
- cost pressures drive a migration of ICT into so-called Infrastructure clouds;
- growing importance of ICT as the critical “nervous system” for socially relevant “smart” infrastructures – such as healthcare, energy, environmental monitoring, or mobility.

Protecting data and services in the cloud is important to governments, organizations and enterprises across all industries, including healthcare, energy utilities, and banking. Thus, the perceived security and dependability risks of cloud computing are limiting its application.

The TClouds project targets cloud computing security and minimization of the widespread concerns about the security of personal data by putting its focus on privacy protection in cross-border infrastructures and on ensuring resilience against failures and attacks.

Objectives & Overall Strategy: Trustworthy Clouds (TClouds) aims to build a prototype Internet-scale ICT infrastructure which allows virtualized computing, network, and storage resources over the Internet to provide scalability and cost-efficiency. The following objectives contribute to achieving the overall goal:

- Identifying and addressing the legal and business implications and opportunities of a widespread use of infrastructure clouds, contributing to building a regulatory framework for enabling resilient and privacy-enhanced cross-border infrastructure clouds.
- Defining an architecture and prototype for securing infrastructure clouds by providing security enhancements that can be deployed on top of commodity infrastructure clouds (as a cloud-of-clouds) and assessing the resilience and privacy benefits of security extensions of existing clouds.
- Providing resilient middleware for adaptive security on the cloud-of-clouds. The TClouds platform will provide tolerance and adaptability to mitigate security incidents and unstable operating conditions for a range of applications running on such clouds-of-clouds.

To demonstrate TCLOUDS, scientists prototype two scenarios involving critical IT-systems including:

- A smart energy grid with Portugal’s leading energy and solution providers Energias de Portugal and EFACEC ENG: A combination of smart metering and a Web-based real-time status and energy consumption control system enables public utility providers to monitor and

efficiently control a public lighting network. TCLOUDS will show how such energy-preserving systems can be migrated to a cloud infrastructure while increasing their resilience, privacy protection and tolerance, from both hackers and hardware failures.

- A patient-centric home healthcare service with San Raffaele Hospital in Milano, Italy, will remotely monitor, diagnose and assist patients outside of a hospital setting. TCLOUDS will demonstrate how the quality of in-home healthcare can be improved cost-efficiently without reducing privacy.

The above objectives are to be achieved within the three main activities as displayed in Figure 1 below.

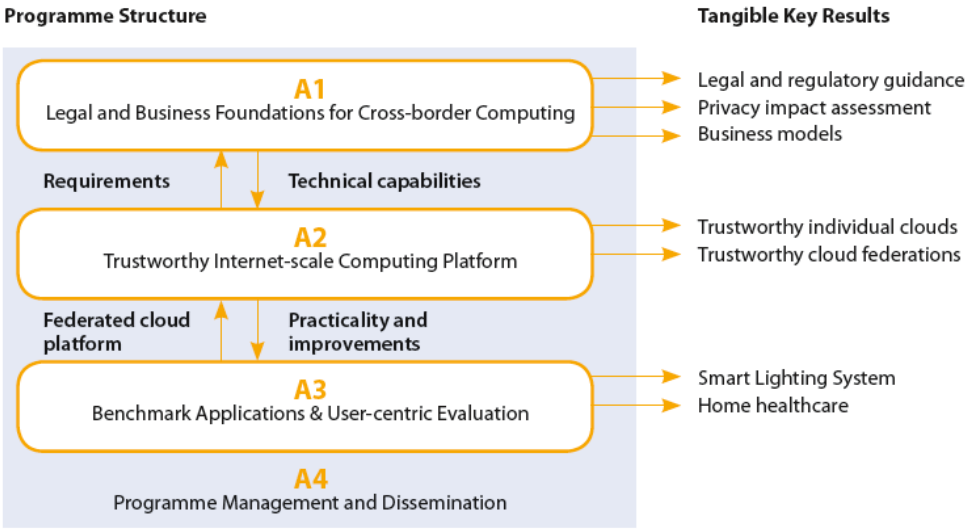

Figure 1: TClouds project activities

The work plan of TClouds encompasses four independently managed activities and twelve tightly integrated work packages.

Description of the work performed and results in the second project period

The TClouds project started in October 2010 and is set to run for 36 months. The work performed within the second project phase in each work package can be summarized as follows:

WP1.1 (Requirements and Roadmap) applies a road mapping approach in order to identify users' requirements towards cloud infrastructure, to help structuring the development of the TClouds technologies, and to determine success indicators of the project in terms of addressing actual requirements and market needs in cloud computing. While originally planned as an activity that would mainly precede the TClouds A2 and A3 developments, it has become redefined in Y2 into an activity that runs in parallel to the TClouds development to produce a better understanding of general cloud security and privacy requirements in the currently evolving cloud market space. A core element of WP1.1 is in this context the set-up of a TClouds online stakeholder community of European experts and cloud providers on the one hand and cloud users – in particular SMEs – on the other hand. The interviewing of these experts has taken place via an online questionnaire. Results are documented in D1.1.5 (extended requirements report) as well as will be integrated in a TClouds white paper. To disseminate these results to a larger audience, a TClouds panel session and a workshop are in preparation at the 2013 CPDP conference in Brussels (Computer, Privacy & Data Protection). WP1.1 is closely integrated into the detailed analysis of the TClouds activity A1 that investigates requirements towards cloud computing from a user- and general community- (WP1.1), legal-(WP1.2) and business-(WP1.3) perspective as well as – as a cross cutting activity – in detail for the 2 TClouds application domains (some results in D1.1.4).

Within ***WP1.2 (Legal Implications and Impact of Cross-Border Cloud Implementations)*** the consortium worked towards an identification of legal implications in respect to cloud computing business and service models. A definition and analysis of the general legal framework and requirements of the European data protection law was made. Moreover, we investigated their relevance to cloud computing scenarios and carved out different ways of achieving data protection compliance (contractual, organisational, and technical). During Year 2 we addressed gaps and

frictions in the current legal framework of the Data Protection Directive 95/46/EC by making suggestions for a revision of this legal framework. Furthermore, the proposed EU Data Protection Regulation is considered with regard to its impact on cloud computing. To counter the legal uncertainties and requirements we identified in D1.2.2 “Cloud Computing: Legal Analysis”, we considered political enablers such as the European Cloud Strategy and established a comprehensive set of contractual topics and rules to adhere to when negotiating cloud computing contracts. We also considered several technical enablers, including recognized certification frameworks and auspicious academic approaches to enhance secure cloud computing using one or multiple clouds. Contributing to WP3.1 we provided a comparison of national laws for two key areas of boundaries for the TClouds health care use-case: Professional secrecy and Restrictions on cross-border transfer.

In Year 1, a first analysis of commercial factors impacting cloud computing (R1.3.2.1.) was completed within ***WP1.3 (Business Impact of and Business Models for Infrastructure Clouds).*** This includes: Cloud Business Case Factors, Cloud Operational Factors, Security & Privacy Factors and Legal & Compliance Factors. The identification of a cloud business model ontology was also carried out and results included in D1.3.1. In Year 2, one of the partners (UMM) departed from the project. Despite this, partners produced internal reports R1.3.1.3 and R1.3.1.4, as well as submitted their findings in deliverable D1.3.2 (“Cloud Computing: Business Impact Analysis”). Deliverable D1.3.2 investigates the impact of various security factors on businesses.

The overall objective of ***WP2.1 (Trustworthy Cloud Infrastructure)*** is to improve the security, resilience and trustworthiness of components and the overall architecture of an infrastructure cloud. In Year 1 the requirements analysis took place mainly in the first year and we also identified the gaps and weaknesses of existing cloud solutions. From there we researched into subsystems and architectures to improve security, resilience and trustworthiness of an infrastructure cloud. During the second year the focus was the consolidation of the requirements and the design of the subsystems and building prototypes. The results of year 2 are reported in D 2.1.2.

The first activity carried on in ***WP 2.2 (Cloud of Clouds Middleware for Adaptive Resilience)*** were the development of a reference architecture for the TClouds ecosystem and a set of design principles for guiding the whole development of the solutions devised in A2. With this architecture in mind, the partners engaged in the development of several sub-systems, from which we like to highlight two. The first one is a Byzantine fault-tolerant state machine replication middleware that can be used to implement intra- and inter-cloud dependable services. During the second year of the project we further improved the quality of our implementation. Our second achievement is the development of theoretical and practical aspects of cloud-of-clouds resilient object storage. The results of this work appeared in a set of publications during the last two years and a prototype will be made available in the next year. Further work on distributed protocols supporting resilience in cloud computing was done beyond these two main achievements; this work is documented in D2.2.2.

WP2.3 (Cross-layer Security and Privacy Management) tackles the problems of security management in infrastructure clouds, in particular in the areas of trust management, federated and distributed security management, and security properties formalization and validation. In the first period, we analyzed technical requirements for security management of infrastructure clouds, in particular also for automated management. Several papers were written and published about this topic. We proposed a novel method for assessing the operational trust in clouds by using an automated audit system. In this period, we consolidated requirements of federated security management and proposed new requirements for large-scale deployments. We designed a new security architecture, protocols and management for secure usage of cryptography in infrastructure clouds. This resulted in a scientific paper that is currently under submission. We integrated trusted computing concepts in the trust management of infrastructure clouds, which resulted in an accepted scientific paper. Furthermore, in the area of distributed security management, we designed and proposed new architectures, protocols, and concepts. This resulted in two accepted scientific papers. Finally, we revised languages and proposed new models for expressing security requirements of infrastructure clouds. A novel approach for automated verification of cloud infrastructures against security policies has been proposed, which resulted in an accepted scientific paper. Overall, WP2.3 is well on track in terms of scientific publications, completing internal results and deliverables. Efforts across work-packages form a tight integration between security components and their management. For instance, the trust management architecture in WP2.3 relies on trusted computing concepts and components of WP2.1.

In ***WP2.4 (Architecture and Integrated Platform)***, the main outcomes of the work done during Y1 are a consistent design of 15 subsystems, including secure block device, cloud of cloud storage, access control and logging and auditing, that will be developed by partners and an initial installation of the TClouds platform Version v0, i.e. an unmodified instance of OpenStack – the selected open source cloud computing framework – on top of which a prototype application from Activity 3 is currently running. All the work for the use cases selection, design of the high-level architecture, draft API and test methodology was done by each partner on his subsystems, following the common methodology shared along the project. Each activity ended with a written report (or activity paper) to consolidate the results, which are collected in the deliverable D2.4.1. During Y2 the main outcomes of the work are: the initial integration of the 15 subsystems (plus one more) into three prototypes (Trustworthy OpenStack, TrustedInfrastructure Cloud and Cloud-of-Clouds - all framed in a single scenario) that form the TClouds platform Version v1; the definition of the test plans for all subsystems and the test results for those subsystems integrated in prototypes; a consistent and automated building and testing system for developing the subsystems being part of Trustworthy OpenStack; finally, the preliminary analysis about the fulfilment of the requirements defined within Activity 1 (the legal ones) and Activity 3 (the application ones) by subsystems and prototypes developed within Activity 2. The work done during Y2 within WP2.4 was organized in phases ended at M16 (technical meeting in Villach), at M19 (integration meeting in Darmstadt), at M21 (technical meeting in Zurich) and at M24. In each phase, one or more activities were carried out, where usually the majority of the partners was involved. Each activity ended with a written report (or activity paper) to consolidate the results, which are collected in the deliverable D2.4.2.

The main objective of ***WP3.1 (Cloud Applications Data Structures for Home Healthcare Benchmark Scenario)*** is to define the cloud based Home Healthcare architecture and specification from the application side of view, to provide technical requirements for cloud computing in the healthcare sector, and to turn this analysis into an architecture, API, and protocols for the client side. This home healthcare architecture will be closely linked and integrated with Activity A2. The WP3.1 results will be validated in collaboration with the demonstrator implementation. WP3.1 starts in M0, and provided its results in D3.1.1 “Trust Model for cloud applications and first Application Architecture” in M12, D3.1.2 “Application API and first specification on application side trust protocols” in M18 and D 3.1.3 “Draft proof of concept for home healthcare” in M24. In the first project year, WP3.1 delivered the cloud-based Home Healthcare use case applications, and developed the mockup based on a commodity cloud Openstack. In the second project year, WP3.1 takes the effort to enhance the integration with the underlying cloud infrastructure from Activity A2 by extending WP3.1 towards the platform layer, by developing a trusted Healthcare Platform as a Service (i.e. the Healthcare T-PaaS). In Year 2, the design and development Healthcare T-PaaS was reported in deliverable D3.1.2 and D3.1.3. Also, WP3.1 organised and participated in several A2-A3 integration meetings with the purpose of analysing and understanding how A2 components can contribute to complying with Healthcare T-PaaS security requirements. In order to guarantee a good alignment between the participants in this work package, we organized partner-to-partner conference calls and technical meetings, organised WP3.1/A3 teleconferences and we scheduled WP3.1/A3 meeting slots during the technical meetings of Lisbon, Turin, Darmstadt, Brussels, Villach and Zurich.

In Year 1, Smart Lighting’s specification, architecture and functional test scenarios were completed and reported in deliverables D3.2.1 “Smart Lighting System Specification” and in D3.2.2 “Smart Lighting System Design” within ***WP3.2 (Cloud-middleware and Applications for the Smart Grid Benchmark Scenario)***. A mock-up of Smart Lighting was defined and hosted at Amazon EC2. Smart Lighting’s integration with A2’s State-Machine Replication (SMR) component was planned. In Year 2, a Smart Lighting prototype was developed and hosted on an OpenStack commodity cloud which was reported in deliverable D3.2.3 “Smart Lighting System Draft Prototype (Prototype)”. Also, we organised/participated in several A2-A3 integration meetings with the purpose of understanding how A2 components can contribute to complying with Smart Lighting System’s security requirements. In order to guarantee a good alignment between the participants in this work package, we had partner-to-partner phone calls, we organised WP3.2/A3 teleconferences and we scheduled WP3.2/A3 meeting slots during the technical meetings of Lisbon, Turin, Darmstadt, Brussels, Villach and Zurich.

WP3.3 (Validation and Evaluation of the TClouds Platform) started in the middle of the second year of project (M18), and provided its first results officially after six months (M24), reported in D3.3.3. In the six months, WP3.3 defined the validation strategy both for the two use cases (realized in WP3.1 and WP3.2) and for the various results of A2. This was necessary because A2 results are of course wider than what the two use cases might need, and to get an objective validation of the project results a comprehensive analysis had to be performed.

The TClouds Consortium

The original consortium comprised 14 partners from 7 different countries. Within the Second Project Period the TClouds Consortium changed: Partners Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) and the University of Maastricht (UMM) terminated their participation in the consortium and left the project. In addition two new beneficiaries, Technische Universität Braunschweig (TUBS)" and INNOVA SpA (INNOVA) became new members.

All newly joining partners are experts in their domains. This partnership of experienced professionals is anticipated to result in a successful project.

TClouds Disclaimer

All public information will be marked with the following TClouds project disclaimer: "This work was partially supported by the European Commission through the FP7-ICT program under project TClouds, number 257243. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The opinions expressed in this deliverable are those of the authors. They do not necessarily represent the views of all TClouds partners."