

*Information and Communication Technologies*

*H2020-ICT-2015*



Secure Container Pilot (SCP)

*– ensuring confidentiality and integrity and ease of use of cloud-based services –*

**Work programme topics addressed:** FTIPilot-01-2016

**Type of action:** Innovation Action

**Coordinating person:** Dr. Martin Süßkraut, SIL  
Email: martin.suesskraut@silistra-systems.com

**List of participants:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Participant organisation name** | **Short name** | **Coun-try** | **Type of  organisation** |
| **1  *Coordinator*** | SIListra Systems GmbH | SIL | DE | SME |
| **2** | SyncLab | SYNC | IT | SME |
| **3** | Exus | EXUS | UK? | SME? |

**Abstract:**

Containers are becoming increasingly popular in private cloud environments. For example, Google alone starts every week more than two billion containers. Containers supports effective software packaging and effective utilization of computers. Modern container engines, like Docker, simplify the composition and management of applications. These features make containers ideally suited to build modern microservice-based cloud native applications.

The security of containers is, however, insufficient when containers from multiple cloud tenants must be protected when running in public or hybrid clouds and even private clouds: software vulnerabilities in the operating system can be exploited to access information in other containers. In addition, service developers must protect the confidentiality and integrity of data against accesses from all other parties, including the public/hybrid/private cloud provider itself.

The new Intel SGX CPU extension introduces the concept of a **secure enclave** which permits to protect code and data from accesses by other software, even when accessed by higher-privileged system software. We will use SGX to build a secure container infrastructure on top of Docker: all data at rest (e.g., on disk), in transmission (e.g., via Ethernet), and during processing (e.g., by a web services) is encrypted and protected from unauthorized accesses.

The SCP project will use these SGX-based secure container technology - which are currently at level TRL3 (experimental proof of concept) and extend this technology to TRL 7 within the duration of SCP. The main objective is to evaluate the technology in an operational environment and ensure that the software satisfies all requirements needed in operational environments. We will evaluate this pilot in the context of three domains: 1) in the context of a logistics domain, 2) in the context of access control system of system administrators, and 3) in the context of a backend banking service.

**Table of Content**

[1. Excellence 3](#_Toc464734798)

[1.1 Objectives 3](#_Toc464734799)

[1.1.1 Market opportunity 4](#_Toc464734800)

[1.1.2 Overall innovation project objectives 4](#_Toc464734801)

[1.1.3 Specific objectives 4](#_Toc464734802)

[1.2 Relation to the work programme 7](#_Toc464734803)

[1.3 Concept and approach 8](#_Toc464734804)

[1.4 Ambition 12](#_Toc464734805)

[1.4.1 Relation to other European projects 16](#_Toc464734806)

[2. Impact 19](#_Toc464734807)

[2.1 Expected impacts 22](#_Toc464734808)

[2.1.1 Alignment with EU strategies and policies 25](#_Toc464734809)

[2.1.2 Assumptions and external factors 26](#_Toc464734810)

[2.2 Measures to maximise impact 26](#_Toc464734811)

[2.2.1 Standardization 27](#_Toc464734812)

[2.2.2 Dissemination and exploitation of results 29](#_Toc464734813)

[2.2.3 Training 31](#_Toc464734814)

[2.2.4 Initial dissemination plans 31](#_Toc464734815)

[2.2.5 Expected exploitable results 32](#_Toc464734816)

[2.2.6 Preliminary exploitation plans 32](#_Toc464734817)

[2.2.7 Management of knowledge and intellectual property 33](#_Toc464734818)

[2.2.8 Research data management plan 34](#_Toc464734819)

[2.2.9 Communication activities 34](#_Toc464734820)

[3. Implementation 37](#_Toc464734821)

[3.1 Work plan — Work packages, deliverables and milestones 37](#_Toc464734822)

[3.1.1 Overall strategy of the work plan 37](#_Toc464734823)

[3.1.2 Timing of the different WPs and their components (GANTT Chart) 38](#_Toc464734824)

[3.1.3 Detailed description of work packages 39](#_Toc464734825)

[3.1.4 List of Work Packages 51](#_Toc464734826)

[3.1.5 List of Deliverables 51](#_Toc464734827)

[3.2 Management structure and procedures 51](#_Toc464734828)

[3.2.1 Management Structure 51](#_Toc464734829)

[3.2.2 Decision making and conflict resolution 51](#_Toc464734830)

[3.2.3 Communication strategy and reporting 51](#_Toc464734831)

[3.2.4 Quality assurance and risk management 51](#_Toc464734832)

[3.3 Consortium as a whole 51](#_Toc464734833)

[*3.4* Resources to be committed 51](#_Toc464734834)

[3.4.1 Summary of staff effort 51](#_Toc464734835)

[3.4.2 Other direct cost’ items (travel, equipment, other goods and services) 51](#_Toc464734836)

# Excellence

SCP will increase the technical readiness level of a **unique secure container platform** to TRL7. This container platform is an extension of the popular **Docker platform**: more than 100,000 applications are running on top of Docker[[1]](#footnote-2). This steep uptake of Docker can be explained by the fact that Docker simplifies the **packaging** and the **deployment** of software. Containers are a virtualization mechanism implemented by the operating system. The are more light-weight than **virtual machines**. However, the security of Docker containers is lacking in comparison to virtual machines: the security of virtual machines are enforced with the help of hardware mechanisms like VT-x, APICv, VT-d and SR-IOV. Contain not only to justify its use in public and hybrid clouds but also in private clouds. SCP addresses this issue by executing containerized applications inside **trusted execution environment**. We use Intel SGX, a novel CPU extension by Intel, that can provide an application with a trusted execution environment which is called a **secure enclave**.

The unique aspect of SCP platform is that it provides **application-oriented security**. Instead of focusing on the security of the hypervisor, the operating system, and the cloud, it ensures the security of an application independent such that it only needs to trust the CPU, i.e., that the trusted execution environment is properly implemented[[2]](#footnote-3). The research on which this work has been based was published in **the** premier systems conference[[3]](#footnote-4).

## Objectives

**Confidentiality, integrity, and availability** of applications and their data are of immediate concern to almost all organizations that use cloud computing. This is particularly true for organizations that must comply with strict confidentiality, availability and integrity policies, including those which process **personal data** and those supporting society’s most **critical infrastructures** such as **finance** and **logistics**.

Until recently, the technological means to protect data while also allowing efficient computation have been limited. A common approach to mitigate the risk of data misuse is to contractually force the service provider to adhere to secrecy. Unfortunately, contractual agreements are ineffective in preventing determined attackers from stealing sensitive information. An example is a recent data breach at a subcontractor of T-Mobile that exposed millions of customers to potential identity theft[[4]](#footnote-5). T-Mobile, together with its subcontractor, is now the target of at least five class action suits related to the data breach. Even though legal delegation of responsibility has merit, it does not address the underlying technical causes of data breaches and identity theft.

With the arrival of novel **trusted computing hardware** on the mass market, in particular Intel SGX[[5]](#footnote-6), it is now possible to secure computation over sensitive data at remote sites. This technological capability is a potential **game changer** considering that limited trust is one of the main inhibitors for outsourcing services to cloud environments as well as to client-owned devices. Intel SGX offers two essential technical contributions: (1) **remote attestation of the application code**, and (2) **confidentiality of data that is processed by the attested code**. SGX achieves data confidentiality by onlydecrypting data inside the CPU package. This approach protects it fromunauthorized access by privileged users, such as system administrators, and isalso resilient to common forms of physical attacks.

### Market opportunity

According to Gartner, the market of IaaS has a size of US$22 billion in 2016[[6]](#footnote-7) and will grow to US$59 billion by 2019. The market size of cloud application services (SaaS) is even bigger with US$37 billion in 2016 and is expected to grow further. The cloud management and security services is with about US$6 billion in 2016 smaller. The objective of the SCP platform is to address three markets: IaaS, SaaS as well as cloud management and security services – which has a total market size of already more than US$65 billion in 2016 and all three segments are growing quickly. We are in particular targeting the growth potentials in these markets which is predicted to have an **annual growth** between 14% and 17% percent.

### Overall innovation project objectives

The SCP platform will be based on an existing secure container prototype (currently TRL3, i.e., experimental proof of concept) that has been developed within the SecureCloud H2020 project. The objective is to commercialize the platform within less than 3 years. To do so, we will

1. Increase the TRL of the **secure container platform to TRL7.** The platform is compatible with the Docker platform. Applications inside of a secure container are, however, executed inside of an trusted execution environment. All files and all communication is encrypted to protect the confidentiality and privacy of all application data and processing.
2. Ensure the security of applications inside of secure containers by **enforcing the memory safety of programs**. Violations of memory safety are the main cause of intrusions like those based on infamous Heartbleed attack[[7]](#footnote-8).
3. Provide **secure container images with guaranteed memory safety for popular applications**. Docker images of applications like **nginx**, **redis**, **postgres**, **mysql**, **mongo**, **gitlab**, **nginx-proxy**, **haproxy**, and **memcached** are very popular and have each been downloaded (i.e., “pulled”) between 5 and more than 10 million times from *dockerhub[[8]](#footnote-9)*.
4. **Implement a business plan that is an extension of the business plan of Docker Inc**. Note that Docker Inc is currently valued at more than 1 billion US$ and its business model is based on service contracts for business customers. Our business model is three fold: a) maintenance contracts for secure container platform (similar to those offered by Docker Inc but for secure containers) and secure container images (see 3) (partner SIL), b) system integrators like SYNC will provide help to other companies to port their applications inside of secure containers, and c) application service providers like EXUS and SYNC will provide the software services inside of secure containers to be able to outsource these into the cloud to facilitate a scalability of their existing businesses without the risk of large hardware investments while protecting the IP and application data.

### Specific objectives

Secure containers are based on Intel SGX. This CPU extension permits to run applications such that all memory state is encrypted such that only the CPU knows the encryption key. Neither the operating nor the hypervisor can access the encryption key nor the state of an application protected with SGX.

Using SGX is, however, not easy. The **performance impact** can between x2 (sequential access) and x2000 (random memory access) slowdown. Since the operating system is not permitted to access the memory of an application, one cannot issue system calls from within secure enclaves. System calls are, however, necessary to communicate with other services and clients. A thread inside a secure enclave must therefore first copy all arguments of a system call to the outside, leave the enclave to perform a system call and then re-enter the enclave (this is a “**synchronous system call**”). This is expensive and hence, we have implemented an **exit-less asynchronous** system call interface that has about an order of magnitude higher system call throughput in comparison to synchronous system calls. This actually enables us to run some services with a higher throughput inside an enclave than outside of an enclave.

Secure containers protect against attacks of an application via the operating system – even if the attacker has physical access to the computer. A hacker has, therefore, to attack applications directly. The attacker could, for example, exploit bugs within the application. To protect against such attacks, we need to ensure the memory safety of these applications. Protecting the memory safety is in general very expensive – slowdowns between x2 to x10 are typical. Using hardware properties of enclaves, we are actually able to reduce the slowdown to about 18% inside of enclaves.

**Secure Container Image Service.** Tuning applications with a competitive performance inside of secure containers is difficult – due to the limitations of the secure enclaves. This requires lots of knowledge and tuning skills. Hence, our objective is to commercialize this knowledge by providing secure container images of popular applications like **nginx**, **redis**, **apache** and **memcached** that are not only well tuned but also provide memory safety using a compiler extension protecting applications inside of enclaves.Access to these images are only granted to customers that pay a monthly service fee. In return, the client gets access to the newest versions of the service, i.e., the client can be sure to get access to the newest versions of these applications with the latest security patches.

**Secure Container Platform**. The SCP platform is based on the Docker platform. The Docker platform itself is open source. To be able to use the newest Docker innovations, we actually do not modify the Docker platform. To ensure that our secure containers are compatible with Docker, we

a) compile the applications such that they can run inside of secure enclaves,

b) encrypt and authenticate all application files that are part of a container image, only an application running inside a secure enclave has the access right (and key) to access these file, and

c) all communication with the enclave is encrypted – not only all TCP connects but also *stdin*, *stdout* and *stderr* streams are encrypted.

We will provide companies with service contracts that gives customers access to the newest version of the secure container platform. The support costs will be the same as those provided by Docker. For example, a **business day support** will cost $1000 yearly per instance, i.e., Docker engine running on a single physical or virtual computer. A **business critical support** will cost $2000 yearly per instance and will include 24/7/365 support.

**Secure Container Cloud Services**. We will provide a private repository for secure containers and managed nodes for secure containers. While the price for secure containers will be on par with Docker (currently, $7 per month for 5 repositories), we will charge more for nodes running secure containers. This will require initially about $150 monthly costs per node instead of $15 monthly per node. This price will, however, need to be adjusted based on real costs and the availability of other clouds offering SGX enabled machines.

**Secure Application Platform and programming language support**. To reach TRL7 and above, we need to gain experience in running a secure container platform and secure applications. Our objective is to port to real-world, existing services inside of secure containers within the SCP project. While the popular container images are mainly written in C and C++ which we already support. However, many modern applications are written in other popular languages like Java, Go, and C#. Within SCP, we will focus on support for **Go** and **C#**. We are aware that Java is very important language but a) the support of Java is difficult, and b) it looks like that within the SERECA H2020 project, RedHat might support the porting OpenJDK to secure enclaves[[9]](#footnote-10). We will focus on one hand on C# since many modern applications are written within C# and the Mono platform[[10]](#footnote-11) supports ahead of time (AOT) compilation of C# programs. This is important for secure enclaves since we want to ensure minimal binaries for performance and security reasons. JIT (just in time) compilers are typically very large and hence, we would like to avoid running a JIT compiler inside of an enclave. On the other hand, we will also support the software written in the GO language inside of enclaves. The Docker platform as well as some popular services like **Consul** are written in GO. The support of GO will permit us to run some critical service like a coordination service (i.e., Consul) as well as certification authorities (part of Docker swarm) inside of enclaves.

**Secure pilot applications**. Within the SCP project, our objective is to port the flagship application of EXUS (i.e., EST) and that of SYNC (i.e., StreamLog), respectively within secure containers. The reasons for moving these applications in secure containers are different. The flagship program of EXUS is EST[[11]](#footnote-12). This was recently awarded as best-in-class globally and is a comprehensive suite of software applications that manages credit risk along the whole lifecycle of accounts, from the moment of disbursement until write-off or debt sale. EFS helps organizations/banks:

* Identify and treat credit risk early
* Perform efficient collections
* Manage legal proceedings and recoveries
* Gain detailed insight into portfolio evolution, collections strategies and resource efficiency

Currently, the product roadmap sees the transfer of **the software to the cloud** in order to facilitate a range of new features as well as a different business model. Clearly, the confidentiality as well as the integrity of the data processed by EST must be protected. There are also the legal requirements that the data of EU banks must not leave Europe. In particular, this must be ensured even if a foreign government would get legal access to all user data hosted by a cloud provider[[12]](#footnote-13). Within SCP, we ensure that all data accessible by the cloud provide is encrypted. EFS is written in C# and our pilot application to show the support for C# application running inside of secure containers.

The flagship application of SYNC is SteamLog[[13]](#footnote-14). This application provides an effective approach for access control monitoring of system administrators. StreamLog audits the actions performed by system administrators to detect abuses. There is an increasing focus on this issue in Italy - as well as in Europe - in the last few years. Already since November 2008, Italian law mandates that abuses by system administrators be detected, the data owners are to be notified and the these administrator be prosecuted in court.

There is a strong business case for porting the security critical parts of StreamLog to a secure container. The main motivation is to protect the **integrity of the collected and logged data**. A malicious system administrator would of course be highly motivated to tamper with the collected as well as with the recorded data. In its current implementation, StreamLog is (at least to some extent) vulnerable to such attacks by a smart system administrator. Hence, we need to protect the data collection and data storage features of the application from administrators with root access. We can do so by executing the collection and storage within secure containers. The presentation layer of the application has only read access to the data and can continue to run outside secure containers.

The parts of StreamLog that run in secure containers will be rewritten in C. StreamLog will be our pilot application to show the support for C-based applications as well as our compiler extension that ensures memory safety of applications running inside of secure containers. Both StreamLog as well as EFS will use the secure container images from SIL for a) a secure database backend, and b) for the secure web servers required to run inside of enclaves to protect the TLS certificates and to ensure the integrity and confidentiality of the communication.

## Relation to the work programme

*Working together, partners with complementary backgrounds, knowledge and skills, and in new and established value-chains, can turn these ideas into sustainable innovative products, processes and services…*

SCP combines partners with complementary expertise and clearly identified contributions to create a unique and new value-chain: SIL provides secure container environment and secure container images, SYNC and EXUS provides software as a service on top of secure container infrastructure complementing their applications with secure container images for web services as well as the data base. There is also large market for helping software companies to move their applications inside of secure containers by a) providing secure container images of standard applications (SIL), and b) providing services to help these companies to port the application for secure containers (SYNC).

*Innovative products, processes and services … address societal challenges … highly competitive in global markets.*

SCP addresses the key societal challenge of increasing the level of protection of organizations against cyber-disruptions, data breaches and theft of critical information. This challenge has been recognized at world-wide level and while today senior executives consider cyber-security as a necessary cost 75%[[14]](#footnote-15), surveys indicate a shift towards 59% considering cybersecurity as a competitive advantage within 3 years.

*Accelerate this commercialisation process by providing extended funding opportunities through an open and agile scheme nurturing bottom-up ideas from innovative constituencies across Europe.*

SCP implements a “go-to-market” scheme. To ensure early exposure and continuous involvement, SCP uses an agile development scheme to create a continuous online testing channel, and incorporates a complete knowledge and collaborative based environment and different incentives to attract both customers and IT Providers to collaborate.

*Supports projects undertaking innovation from demonstration stage to market uptake, including piloting, test-beds, systems validation in real world/working conditions, validation of business models.*

SCP will develop an innovative secure container platform that will be demonstrated and demonstrated in operative environments. This will become a market-ready platform by the end of the project. The pilots and the evaluation will permit us to evolve the current prototype in the direction required by the market.

*It targets relatively mature new technologies, concepts, processes and business models that need a last development step to reach the market and achieve wider deployment*.

SCP starts from an existing prototype and existing secure container images at TRL3 and will move these to TRL7. The detailed table is provided in Section 1.3.

*Proposals must relate to any field under "Leadership in enabling and industrial technologies" and/or to any of the specific objectives under the priority "Societal challenges".*

SCP focuses on improving cyber-security for SMEs, directly related to the *Secure Society Challenge* and more specifically to the specific aim *Cyber Security for SMEs, local public administration and Individuals.*

## Concept and approach

### Overall Concept

Commercial approaches either cover only the secure storage of encrypted data within the cloud, and thus do not allow for any processing of that data within the cloud. Our approach utilizes novel cryptographic hardware found in upcoming commodity CPUs—in particular, Intel SGX.[[15]](#footnote-16) This kind of hardware allows the execution of encrypted code on encrypted data where the corresponding plaintexts are only known inside the processor but will never leave it. The secure area in which the processing of the plaintext data happens is referred to as an “enclave”.

Current commercial products for SGX are so far limited. Microsoft supports secure enclaves within Windows but does not support paging – limiting enclaves to only about 90MB. Intel provides a SGX driver for Linux that supports paging. In this way, enclaves can be up to a size of 64GB. Paging introduces some overhead. In case, programs have good locality or mainly sequential accesses, overheads can be kept to a factor of x2. It is expected that the next generation of Xeon CPUs will have a much better support for enclaves, in particular, these enhancements will reduce the paging frequency and hence, the runtime overheads.

Intel supports a SDK (software development kit) to build applications for secure enclaves. The idea of this SDK is that only parts of an application should be stored inside an enclave. For new applications, this seems to be an acceptable approach. However, splitting existing applications in two parts (data+ code inside an enclave and data+code outside of the enclave) is a very difficult challenge. This partitioning introduces performance overheads for entering and leaving the enclave and hence, one wants to limit such enclave transitions. Even more difficult are the security challenges such a partitioning introduces since one defines a new interface inside an existing application that provides access to the data and code kept inside of an enclave. Such a reengineering existing applications has proved to be an extremely difficult endeavor since, for example, often classes would need to be split in two – to keep the security relevant fields of an object inside an enclave and the remaining data outside.

In contrast to the existing approaches, we support that a complete application will be executed inside an enclave. This eliminates the need to define a new interface of an application. In particular, we will support many popular applications can run inside of enclaves without reengineering. However, these applications need to be properly configured to ensure security and properly tuned to ensure sufficient performance. Often, both require intimate knowledge of these applications. To simplify to execution of such applications, we will provide a **container image service**. Popular service like **nginx**, **apache**, and **mysql** will be properly configured inside of a secure container such that all communication is encrypted (via TLS), all files are encrypted before leaving the enclave, and these applications are executed inside of an secure enclave.

Secure versions of popular applications will be provided in form of secure container images. Customers can configure and operate instances (i.e., containers) of these secure images only after signing up to a paid subscription services.

The secure container will run on top of operating systems. They are protected against attacks from/via the operating system (these are called **iago** attacks) by a) encrypting data to be stored on disk or transmitted via the network, b) performing all memory management of the application inside the enclave (required to protect against iago attacks), and c) performing a careful checking of all arguments of calls to the operating system.

Secure containers are also protected against attacks by hackers. Attacks on applications frequently use low level vulnerabilities like buffer overflows and return oriented computing. For example, the OpenSSL Heartbleed attack used such low level vulnerability of OpenSSL[[16]](#footnote-17). We have a compiler-based approach that protects applications inside of enclaves with minimal overhead (average is below 20%). This protection will only be available for enterprise subscriptions.

Secure containers are not only protected against accesses from system administrators, cloud providers and operating systems but also against low-level attacks by attackers with knowledge of application bugs that violate memory safety – which are the most common attacks. (This feature will require an enterprise-level subscription)

An application running inside a SGX secure enclave will suffer non-negligible performance overheads if its working set does not fit inside about 90MB[[17]](#footnote-18). We will provide a mechanism (with enterprise-level subscription) that extends the supported working set size of applications by automatically keeping some state outside of the enclave.

Our compiler extension can transparently move application state of an application outside of a secure enclave. This mechanism is faster than the hardware mechanism since it use the actual object size instead of page size (which is 4KB). (This feature will require an enterprise-level subscription)

We will investigate the secure container approach in the context of two pilot applications. These pilot application will run as secure containers and will access standard secure container applications like **redis** and **mysql**, respectively.

### Strategy and approach

Our strategy to ensure the success of SCP is that we focus on the following properties:

* **Ease of use**. SCP is based on well known concepts like Docker containers and images. Also a Docker infrastructure is usable. The main complexity of the SCP approach is hidden in the generation of secure container images which are made available via a **subscription service**.
* **Security**. Applications will need to run in open systems like public clouds and might even stretch across multiple clouds for availability and scalability. SCP protects the confidentiality and integrity of applications using not only secure enclaves but also compiler extensions that protect applications against attacks. The compiler extensions are only available to **enterprise-level subscribers**.
* **Manageability**. Considering that applications will run across multiple clouds, one needs tools to simplify the management of these applications. Hence, SCP supports integration of secure containers within Docker Swarm to simplify the management of secure containers. Integration with Docker swarm requires an **enterprise-level subscriptions.**
* **Transparency.** Enterprise-level subscriber can get access to all source code that runs inside of enclaves via an additional **source-code subscription**. This subscription does not include the compiler that is used to protect and speed-up the execution of applications inside secure enclaves.
* **Ease of adoption.** To ensure to potential customers can simply try out secure containers, we will have a free tier that includes

The two pilot applications allow us to integrate two flagship applications inside of secure containers. This facilitates us to learn …

## Ambition

Although cloud computing models offer several economic advantages compared to on-premise solutions, many enterprises are still reluctant to move their mission-critical applications and data to the cloud. One reason for this reluctance is the lack of trust in the security solutions offered by the cloud provider and the effort and skills needed to move applications to the cloud.

The SCP project provides a platform that simultaneously establishes trust and offers competitive performance through the use of secure containers. No commercial offering is so far available that provides similar features as the SCP platform. SCP extends a modern container-based execution environment (Docker and Docker Swarm) and facilitates companies to move applications to the cloud not only by protecting the application but also by providing prepackaged secure container images for standard application components like the web service and the data base.

We also explain how the SCP project will advance the state-of-the-art in the following areas.

**Challenge: Secure container-based application provisioning**

As discussed in Section 1.1.3, the traditional model of running applications inside of virtual machines has several drawbacks: first, the acquisition of new resources through virtual machines introduces a non-negligible latency, making it impractical for applications that require low latency for the provisioning of new resources; second, running virtual machines including the full OS stack for potentially each micro-service introduces unnecessary complexity and runtime overhead. Other approaches to reduce the application’s size, for example, library operating systems [20] or customised language/runtime systems[[18]](#footnote-19) require the developer to adapt the application.

**SecureCloud will follow a container-based approach using the Docker framework. Docker-based application containers are orders of magnitude smaller and less complex than full virtual machines, which will therefore serve as the interface between the user’s application in form of a micro-service and the underlying software and hardware stack. The container-based approach provides greater flexibility to customers: application containers can be launched and restarted significantly faster than virtual machines. Containers are also a good match with a secure micro-service execution environment because of the need for a lightweight mechanism to host the potentially large quantity of micro-services.**

With regards to the implementation for the application containers, we identified Docker as a technology satisfying our requirements best. Since the project consortium comprises partners, such as CloudSigma, that have used similar techniques for their own products, we are well-positioned to employ Docker in a way that allows us to realise a **secure execution context**. To show why Docker suits best our needs, we compare it to related projects and approaches recently evolved:

* ***Virtual Machines (VMs)*** are the de-facto standard to partition and isolate applications in today’s cloud data centres. VMs are generally regarded as more secure than containers because of the strong isolation of VMs by the hardware instead of operating system-based isolation as in containers. However, in terms of resource usage and performance, VMs are heavyweight. Lightweight alternatives with similar levels of security would be preferred in many typical use cases.
* ***Docker*** allows to deploy services inside of lightweight software containers. It provides an additional layer of abstraction by virtualizing the underlying Linux operating system. This includes resource isolation through *cgroups* and kernel namespaces. Moreover, multiple containers can be run within a single Linux instance avoiding the overhead typically associated with virtual machines.

**In SecureCloud, we will improve the security of lightweight containers as provided, for example, by Docker. In doing so, we combine the leanness and efficiency of containers with the security levels previously only achieved by heavyweight virtual machines. The container provides the runtime environment, which is encapsulated within an enclave to guarantee security. We will also seek to integrate secure containers with major cloud management software, such as OpenStack, to make our technology easily available to a wide audience.**

**Challenge: Secure Cloud Storage**

Besides computing and communication resources, big data applications running on the SecureCloud platform will need secure storage. Cloud storage solutions have become a commodity for commercial users over the last years. These services provide a wide range of advantages, from allowing users to manage files over different devices, to simplify collaboration among colleagues, and even to simply back up personal data.

Using a single cloud, however, has a series of drawbacks: first, a cloud is still vulnerable to outage due to system overload or failure; second, storing the entire data in a single cloud brings forth data privacy issues if the system is compromised by an attack or by governmental laws that force the provider to release a user’s data [21]; and third, there is typically a large latency inherent to interacting with clouds that are far away from the end devices. Spreading the content over multiple clouds or storage devices forces attackers to compromise multiple clouds in order to gain access to the data. The use of network coding as a base technology makes this process not only seamless, but allows the user of the system to decide how much protection against failures is available and provides a natural encryption mechanism over the data.

In the context of distributed storage, network coding was originally proposed for sensor networks [22] and research has focused primarily on the problem of code regeneration [23]. There has also been a lot of research in creating codes for data centres with focus on limiting local data transfers due to failing nodes. Facebook introduced Locally Repairable Codes [24] to minimize repair bandwidth, and Windows Azure Storage employs Local Reconstruction Codes [25] for the same purpose.

An inherently different approach from previous network coding research focuses on exploiting commercial systems with inherently heterogeneous characteristics (e.g., round-trip delay, throughput, storage cost) to provide improved services to the end-user. Using network coding to allocate resources in a flexible manner in the clouds, was shown to increase the download speed for end-users, while providing security (data privacy) guarantees. More specifically, this approach stores data in a network coded fashion on distributed storage entities, e.g., Dropbox, Box, Skydrive, or Google drive. Network coding stores different linear combinations of the original data in each cloud, which allows us to avoid an overwhelming book-keeping process when downloading the data and also to avoid additional delays from a highly loaded cloud.

**Network coding acts as a natural cipher on the data with high security guarantees. SecureCloud will require a suite of stronger and more advanced data privacy mechanisms to trade-off computational complexity of the privacy mechanism and the level of protection provided is key to manage different type of devices, data types, and data requirements. SecureCloud will deliver this suite of privacy methods and deploy it as part of its Cloud storage framework. The starting point will be CCloud’s Secure Any Cloud Aggregator to easily deploy these privacy levels using any commercial cloud or storage device. CCloud will make available its software solutions as part of SecureCloud, develop a suite of security solutions with different computational requirements and protection levels, as well as develop new solutions for the benefit of SecureCloud’s platform and to enlarge CCloud’s product offering into the future.**

### Relation to other European projects

Several European projects are linked to SecureCloud. They complement and/or can provide input for the design and development of the SecureCloud. They are listed in the following table.

|  |  |
| --- | --- |
| Related EU project | How SecureCloud extends beyond |
| The SERECA[[19]](#footnote-20) project focuses on secure reactive programming in public clouds without relying on security mechanisms of cloud providers. SERECA does not address big data processing. | The focus of SecureCloud is on secure big data processing in the context of critical infrastructures. SecureCloud will use the system software developed within SERECA. SecureCloud extends it by using **containers,** support for **dependability** and **big data processing**. SecureCloud will use a micro-service approach with a typesafe, compiled language to reduce the size of the trusted computing base instead of including a complete Java Virtual Machine (JVM) in the trusted computing base as SERECA does. |
| The SafeCloud project proposes a cloud infrastructure to protect against malicious operations over user data across all levels of the data stack management. | The SafeCloud project shares some of the goals of SecureCloud, in particular, with respect to secure computation against non-trustworthy cloud providers. It focuses, however, on data storage, does not consider hardware extensions, and supports security only by the means of cryptographic software techniques. In contrast, SecureCloud uses hardware extensions of commodity CPUs for speed and confidentiality. |
| A4CLOUD[[20]](#footnote-21) provides methods and tools through which cloud stakeholders can be made accountable for the privacy and confidentiality of information held in a cloud. These methods include risk analysis, policy enforcement, monitoring, and compliance auditing. | By aiming at accountability through policies and supervision, A4CLOUD assumes generally cooperative stakeholders. Thus, it differs from SecureCloud’s approach of guaranteeing security in spite of untrusted cloud providers, system administrators and partially, untrusted software developers. |
| Contrail[[21]](#footnote-22) develops an integrated approach to virtualisation, offering Infrastructure-as-a-Service (IaaS) mechanisms, services for federating IaaS clouds, and Platform-as-a-Service (PaaS) support on top of federated clouds. | Contrail focuses on a service stack that integrates different types of clouds into a federation. In contrast, SecureCloud focuses on the dependability of applications and secure big data processing. In SecureCloud an application might run across multiple clouds to increase the application dependability but there is no focus on supporting cloud federation. |
| LEADS investigates a large-scale data-as-a-service (DaaS) approach, which gathers, stores, and processes data across multiple micro data centres. | LEADS and SecureCloud are complementary: LEADS focuses on a new *data-as-a-service* (DaaS) and data mining algorithms, while SERECA targets how to ensure the confidentiality of big data processing. We will incorporate results of LEADS into SecureCloud. |
| MODAClouds provides methods, frameworks, and tools for the design, implementation, and deployment of model-driven applications on multiple clouds with guaranteed QoS. Quality assurance during the application life-cycle is provided through optimisation of chosen model parameters. | By targeting federated clouds, MODAClouds aims to provide a common abstraction across heterogeneous clouds, masking provider differences. In SecureCloud, we assume that clouds provide the same API - either by using a federation approach or by using standard API endpoints (e.g., all clouds use the OpenStack API). |
| CloudCert[[22]](#footnote-23) supplied a test-bed framework for integrating mechanisms that coordinate the exchange of information related to security aspects. | CloudCERT wants to support information exchange and mainly addresses cyber attacks from the outside. Compared to SecureCloud, it has a different focus, but can make use of its security mechanisms. |
| CUMULUS[[23]](#footnote-24) developed an integrated framework of models, processes and tools supporting the certification of security properties of IaaS, PaaS and SaaS services in clouds. | CUMULUS aims at certifying security properties and not at developing and implementing a new platform such as SecureCloud. However, the results of SecureCloud could be certified using the CULUMUS framework. |
| PASSIVE[[24]](#footnote-25) proposes a policy-based security architecture for the specification of security provisions, including fine-grained control over device access. The system for authentication of hosts and applications should support separation of concerns, such as policing and judiciary. | PASSIVE focusses on policies and access control, and it does not aim at providing security along the processing chain, as is the goal of SecureCloud. Results from PASSIVE may be integrated in SecureCloud to solve authentication issues. |
| PRACTICE[[25]](#footnote-26) focusses on cryptographic mechanisms that allow for distributed computation of arbitrary functions of secret inputs, while hiding any information about the inputs to the functions. | In contrast to SecureCloud, which strives to protect code and data in memory by embedding it in secure enclaves, PRACTICE focuses on the processing of encrypted data. This does not protect application code, so the approach and expected results differ from SecureCloud. SecureCloud could include results from PRACTICE as an additional security mechanism. |
| SECCRIT[[26]](#footnote-27) analyses and evaluates cloud computing technologies with respect to security risks in sensitive environments. It develops methodologies, technologies, and best practices for creating a secure, trustworthy cloud computing environment for critical infrastructure IT. | SECCRIT wants to develop security guidelines, policies, and best practices, so it approaches security at a theoretical level. It does develop a prototype platform or technical framework, offering protection of code and data against untrusted cloud providers, and it ignores performance considerations. |
| SECFUNET[[27]](#footnote-28) designs and develops a coherent security architecture for virtual networks and cloud access. Key aspects are an identification scheme, an authentication system, isolation of virtual networks, and access control mechanisms. | SECFUNET focusses on data access and not like SecureCloud on protecting data and code while being processed. In contrast to SECFUNET, SecureCloud also considers performance aspects. |
| TClouds[[28]](#footnote-29) developed an advanced cloud infrastructure for computation and storage, which aims to achieve security, privacy, and resilience while still being cost-efficient, simple, and scalable. | The goals of TClouds are similar to that of SecureCloud but it uses an orthogonal approach – in particular, it is not using hardware extensions. The techniques of TClouds can be applied to SecureCloud to increase service security. |
| TRESCCA[[29]](#footnote-30) provides a secure cloud platform by using both hardware security (i.e., System on Chip (SoC)) and virtualisation techniques to ensure the security of edge devices. It contributes to existing legacy solutions by adding non-intrusive add-ons. | TRESCCA focuses on the development of secure set-top boxes, possibly realized as migrating VMs, where client tasks (e.g. credit card payments) can be offloaded from the cloud to be executed in a trusted environment. In contrast to SecureCloud, it does not offer secure data processing in the cloud, and users still have to trust the cloud software stack. |

To disseminate the ideas to be developed in SecureCloud, we already established initial contact with related projects, mainly targeting projects most closely aligned to SecureCloud. As a result, we plan to have close collaboration with SERECA, SafeCloud, and LEADS as follows:

* TU Dresden (TUD) and University of Neuchatel (UniNe) participate in the LEADS project, which focuses on the efficient and cost-effective processing of big data. However, LEADS does not focus on the confidentiality aspects. There will be close collaboration, information exchange, and integration of integrating results of LEADS into SecureCloud.
* TU Dresden (TUD) and Imperial College (IMP) participate in the SERECA project, which addresses secure cloud computing by enabling reactive programs to be executed securely in the cloud. SERECA will develop system software to support the execution of JVM-based reactive programs in the enclaves. We will reuse the lower-level system software developed by SERECA that is not specific to the JVM.
* Imperial College London (IMP) is a partner in ModaClouds and can thus contribute research results from the model-driven view for cloud federation proposed by the ModaClouds.
* University of Neuchatel (UniNe) participates in the SafeCloud project, which investigates a cloud infrastructure to protect against malicious operations over user data across all levels of the data stack management. We will integrate some of the results relating to secure storage of the SafeCloud into SecureCloud.

# Impact

According to Cisco’s Global Cloud Index Forecast, more than 30% of the cloud workloads will be in public cloud data centres by 2018. They expect the workflows in clouds to nearly triple between 2013 and 2018, while the workload of traditional data centres is expected to decline in the same period. If less than 40% of the Internet consumer population used cloud storage in 2013, by 2018, 53% of this population should be using it.[[30]](#footnote-31) Goldman Sachs expected that spending on cloud computing infrastructure and platforms should grow at a 30% CAGR from 2013 through 2018, while overall enterprise IT should grow only 5%. They see spending in cloud infrastructure and platforms growing to $43 billion in 2018, in a global market for enterprise information technology that is larger than $300 billion.[[31]](#footnote-32) According to Network World, security (36%), cloud computing (31%) and mobile devices (28%) are the top 3 initiatives IT executives are planning to have their organizations focus on over the next 12 months starting on 2015.[[32]](#footnote-33) According to Ovum, by 2016, 75% of EMEA-based enterprises will be using IaaS with investments in private cloud computing showing the greater growth.[[33]](#footnote-34)

Europe is facing a crossroad regarding cloud adoption and security. SecureCloud aims to provide solutions for these cloud security challenges. The Forrester Forecast estimated that global SaaS revenues should reach $106 billions in 2016 (21% increase over projected 2015 levels). This includes an increase from $9 billion in 2013 to $16 billion in 2016 in security.[[34]](#footnote-35) A report from security and governance firm Skyhigh Networks[[35]](#footnote-36) provides evidence demonstrating that European enterprises use an average of 588 cloud services with just 9% providing enterprise-grade security capabilities and the remaining 91% posing a risk. Of the total 2,105 cloud services used by European enterprises, only 12% encrypt data at rest, 21% support multi-factor authentication, and 5% are ISO 27001 certified. The report also warns that shadow IT is “widespread and uncontrolled” and is 10 times more prevalent than companies assumed.

As explicitly emphasized in the Excellence section of the proposal, dependability (confidentiality, integrity, availability and security) of applications and their data are of immediate concern to almost all organisations which use cloud computing, and particularly to organizations that must comply with strict confidentiality, availability and integrity policies, including those supporting society’s most critical infrastructures, such as smart grids and utilities in general, health care, and finance. Hence, there are a number of application domains that represent major business drivers for a massive take-up of dependability-enhanced cloud technology, such as the one being developed by SecureCloud. In the following, we briefly comment on some of such drivers, and provide factual data about market forecasts for each of them.

The Infrastructure-as-a-Service market in Europe is expected to grow quickly over next few years. The main factor accelerating this growth rate is widely considered to be the comparable cost effectiveness. According to a forecast by International Data Corporation (IDC), worldwide spending on public infrastructure will reach $107 billion by 2017 having a compound annual growth rate (CAGR) of 23.5%, five times greater than that of the entire IT industry. Information technology research and advisory firm Gartner group forecasts similar results, predicting IaaS spending growth of 19% CAGR. Gartner’s research suggests cloud computing is fast becoming the bulk of new IT spending and should dominate by 2016. They predict that by 2016 private cloud will begin to give way to hybrid cloud with nearly half of large enterprise having hybrid cloud deployments by the end of 2017.

While the forecasts presented above are generally considered positive growth, concerns about data security and privacy whether perceived or real are still seen as the main inhibitors of cloud adoption. Various government agencies and local municipalities collect, store and manage large amounts of data from closed circuit cameras, traffic cameras and traffic lights as well as from sensors for alerting first responders to emergencies such as fires and road accidents. There are various levels of authentication needed to be able to access and process this data which is being collected by diverse sources such as Internet of Things (IoT) devices. While some data may be public (e.g., traffic delays or road works information), a large amount of data will contain sensitive information and therefore will require secure storage and multi-level access policies. For example, privacy invasive tools such as face-recognition and detection tools will require much more stringent policies on access and use. Such tools, used for law enforcement, will no doubt require a much higher level of security and encryption as well as greater processing power and higher availability. Data may also need to be shared between government agencies and/or local municipalities, each requiring their own level of authentication. Data portability will also play a big part while public services begin to move private datasets into the cloud, and make them accessible to legitimate users in a secure way.

A major field of application of dependability-enhanced cloud technology—and, not by chance, the main reference domain of the project—is cloud-based smart grid monitoring and control. Remote monitoring and control of a critical infrastructure (CI) such as the smart grid requires an expensive ICT layer and data centre infrastructure for tasks as maintenance, system updating, and hardware provisioning. Operating and maintaining such an infrastructure lies outside of the core competences of most CI operators. A cloud deployment model is therefore an attractive proposition because it would enable CI operators to migrate the bulk of the data collection and processing to an externally managed cloud environment. In particular, the security approach chosen by SecureCloud is ideally suited for providing dedicated yet cost-effective solutions to CI applications.

Evidence is demonstrating that Critical Infrastructures are vulnerable to cyber-attacks, and that such attacks will increase dramatically in the future.[[36]](#footnote-37),[[37]](#footnote-38),[[38]](#footnote-39),[[39]](#footnote-40) From April 2014 to April 2015, outage in large-scale providers varies according to the specific service. For example, cloud storage outages worldwide for large Cloud services range from 7 outages (~8 mins total) for HP Cloud Object Storage and 13 outages (~18 mins total) for Google Cloud Storage to 29 outages (~3 hours) for Amazon S3.[[40]](#footnote-41) Cloud computing services have had outages ranging from around 1h for Amazon EC2 and around 10h for Rackspace Cloud Servers and the Google Compute Engine to around 45h for Microsoft Azure Virtual Machines.

Regrettably, with current state-of-the-art technology, cloud-based CI monitoring and control is impossible due to several security limitations of currently available cloud platforms and solutions, some of which are briefly commented in the following.

A first limitation is the limited data security. Critical decisions are taken based on the measurement data provided by a monitoring system. This implies that data confidentiality and integrity are of primary importance. Today’s cloud platforms lack adequate guarantees that would be acceptable to CI operators. The secure enclaves concept of SecureCloud can offer such strong guarantees.

A second limitation is insufficient guarantees in terms of service availability and responsiveness. A timely response of detected problems in the critical infrastructure is an important requirement, e.g., to have human operators react quickly to critical conditions such as a terrorist attack. The mechanisms enhancing availability and timeliness that SecureCloud will develop can solve this problem.

A third limitation is limited service isolation. As a critical infrastructure, any system associated with the critical infrastructure must comply with a variety of regulations and standards. Validation of compliance is a complex and expensive process though, especially, when third-party cloud providers are involved. With the trust of the SecureCloud cloud platform rooted in secure commodity hardware, such compliance validation will be simplified substantially.

Last but not least, when it comes to cyber and cloud security research, the economic impact should be measured in terms of the cost of not implementing ICT security solutions. This is rather difficult to measure, but it is also well known to have a negative impact on service provision, business revenue, costs and public image. Risk managers worldwide try to estimate the potential damages of security incidents. For instance, it has been calculated that the macroeconomic costs of a major disruption of critical infrastructure in Switzerland, with an annual GDP of CHF 482 billion (EUR 464 billion) are estimated at CHF 6 billion (EUR 5.8 billion), or, 1.2% of GDP. Along with many other research initiatives aimed to address challenges in cloud security, a domain that is clearly in high demand, SecureCloud brings a unique and novel approach to this problem and aims at creating a significant impact in this respect.

Cloud-based security services represent an emerging market with rapid growth. It is estimated to rise to $3.1 billion in 2015 and expected to hit $4.13 billion by 2017. Gartner forecasts that two of the top three most sought cloud services will be web security services and identity and access management (IAM), two of the core topics addressed by SecureCloud. Managed Security Services (MSS) are driving adoption of cloud-based security services among enterprises. MSS delivery models are in turn being affected by demand for cloud-based security services, which is enabling security providers to become de facto MSS players. According to Gartner, multi-function Identity as a Service (IDaaS) will see significant growth. IDaaS is described as a combination of administration, authentication, authorization and reporting functions. Identity and access management is also seen as one of the key areas to manage SaaS. Gartner has also identified recently in their report “Five styles of Advanced Threat Defense” the following techniques to fight them: 1) Network traffic analysis, 2) Network forensics, 3) Payload behaviour analysis, 4) Endpoint behaviour analysis, and 5) Endpoint forensics. The superior data dissemination features and secure processing capabilities that will be brought about by SecureCloud will represent key enabling factors of the aforementioned five techniques/activities. In summary, SecureCloud is very timely and it will target—with respect to this specific application domain—a market estimated to reach $4.13 billion by the end of the project with a significant growth potential.

Another major field of application of security and dependability-enhanced cloud technology is e-health applications. The size of the e-health market varies significantly, depending on the methodology and definition of what can be classified as e-health. Estimates from recent market reports range between $96 and $160 billion per year, with growth rate in 5 years between 12% and 16%. In particular, m-health—which is an important niche of the e-health domain that massively relies on cloud computing—is forecasted by the promoters of the Mobile World Congress to reach in the US a total size of $25 billion by 2017. As side effects, m-health applications might bring to mobile phone operators a total revenue of 11,5 billion dollars by 2017, to mobile device vendors $6.6 billion, to application and content providers $2.6 billion, and to other stakeholders of the health domain $2.4 billion by 2017.[[41]](#footnote-42)

Brazilian utilities usually use big data centres in order to store data from AMI (Advanced Metering Infrastructure) and AMR (Automatic Metering Reading) systems. Those data centres store and process all data collected from smart and regular meters. They are known as MDM (Metering Data Management) systems and, in general, refer to centralized and regular energy meters installed in large customers with some kind of remote communication. These MDM systems are responsible for the billing and implement specific algorithms for fraud detection, energy balance, energy delivering and fault detection, load shedding, among others. As the collected data are used to compute utility bills, metering applications of MDM systems are very sensitive: security concerns are serious, since an attack can compromise the utility income source.

Frauds in energy meters, as well as in other metering systems (gas, water) can, in certain Brazilian regions, reach over 25% of the delivered amount. Therefore, security and fraud detection became a major concern of utility companies deployed in those regions. Also, specific integrator companies usually supply most hardware and software infrastructure for MDM systems. In this way, distribution utilities tend to have a centralized hardware and software system installed in-company, with security specifications through service contracts between the utilities and the system integrators.

Smart metering, as well as many other applications, follows the current tendency towards cloud adoption. Clouds can be used to distribute the computational effort to run all processes needed for smart metering applications, with the big advantage of greater scalability and the distributed cost of hardware. However, the security concerns remain, once smart metering applications are very sensible, unauthorized agents should not access data and processes. Therefore, SecureCloud intends to create and validate privacy and security for cloud computing applications that can provide and ensure the safety of data and processes that run sensible applications, using real data and applications from smart grid pilots as applications for validation.

## Expected impacts

The outcomes of SecureCloud project will produce breakthrough solutions for cloud computing service providers with the current (insecure) cloud service composition as well as the user of such services. The current situation is inappropriate for the applications currently deployed because it solely relies on the cloud provider’s reputation concerning security. Therefore, the current service market in Europe is not able to sustain the evolution of a widespread ecosystem of cloud services because it lacks the security levels required to execute such services.

We foresee the SecureCloud research results to be deployed within 2 to 5 years after the project completion. It can be even shorter as cloud computing services are catalysts for sustainable developments in Europe. These deployments are associated with the need of organisations to share knowledge, resources and work towards common business goals.

In Europe, the possible set of shared resources between organizations should not be restricted to cloud storage or computing, but must include service elements as the building blocks of such services. The secure virtualized infrastructure of SecureCloud and its management solutions represent a fundamental opportunity in the European regulatory framework to strengthen the position of cloud computing providers delivering services. With strong business cases for more secure access of infrastructures from service developers and providers facilitated with programming environments supporting open and standard interfaces, SecureCloud will impact how developers design their next generation systems to be deployed on the Internet, and how companies offer new services.

With the results expected by SecureCloud, cloud service platforms enabled with secure enclaves will support current sensitive business and government applications such as healthcare, critical systems, banking, and voting. Considering its impacts on the European society and the rise of a corresponding service market, it is fundamental for European cloud infrastructure and service providers to lead the definition of new service platform technologies.

SecureCloud will develop novel technologies in cloud computing, addressing several challenges proposed in the Horizon 2020 Work Programme for Leadership in enabling and industrial technologies in Information and Communication Technologies, especially those listed in the coordinated call with Brazil H2020-EUB- 2015. In this section, we enumerate the expected impacts in the call and the contributions of SecureCloud addressing these impacts.

**Expected impact**: *Development of technologies integrating cloud and big data in terms of architecture, middleware and services.*

* **Contribution**: Advance state-of-the-art technologies for detailed QoS monitoring and enforcement.

The cloud elasticity can be nullified by the lack of suitable adaptation mechanisms. A middleware that offers detailed monitoring and highly responsive orchestration services that work seamlessly together will provide mechanisms for building both applications and platforms that can react quickly to a changing environment and, thus, can enforce specified Quality-of-Service metrics. This will be possible through an intelligent system that not only collects a rich set of metrics in a detailed fashion, but also processes the high-volume low-level data to generate meaningful actionable information.

* **Contribution**: In SecureCloud, we address dependability, confidentially and integrity by introducing micro-services that run inside of secure containers.

The micro-service abstraction allows a much wider adoption of cloud services compared to traditional IaaS offerings as customers can focus on data analytics and business logic leaving out the burden of maintaining explicitly an infrastructure in form of virtual machines to run services. In contrast to existing service offerings such as Amazon Lambda, the micro-services provided through SecureCloud are dependable and run in secure containers, thus increasing the trust of the user in the cloud provider and allowing a wider adoption of cloud technologies.

* **Contribution**: The implementation efforts taken in the SecureCloud platform will be contributed to the open-source OpenStack technology, hence increasing the customers trust in that technology.

The use of open-source technologies for cloud service offerings such as the SecureCloud platform allows a wider adoption of cloud technology as it increases transparency of the implementation for the underlying software stack, and provides trusted security when using secure micro-services due to their reliance on secure containers. Moreover, the use of open-source technologies allows a close collaboration with existing communities and provides a close feedback loop.

* **Contribution:** The consortium will develop the appropriate use cases for demonstration of SecureCloud platform capabilities to improve the competitive position of the European cloud sector on example of smart grid critical infrastructure.

The smart grid critical infrastructure is a target of different cyber attacks therefore the consortium will demonstrate that the SecureCloud platform can improve the assurance of computing techniques for Smart Grid applications.

* **Contribution**: Cloud data privacy by design.

SecureCloud combines secure processing with secure data storage developing cutting-edge techniques for data privacy by spreading stored data over multiple cloud providers. These capabilities are key for sensitive data, ranging from end-users' personal data, to personal sensor/location data and home smart metering. These new capabilities, developed as part of SecureCloud's WP4, provide a unique market offering for EU's SMEs to impact the Cloud security sector, which is set to increase its yearly investment from $9 billion in 2013 to $16 billion in 2016. This is also particularly interesting as the cost for lost/compromised personal data/record in 2013 amounted to an average of $145 per record, with companies in the United States losing the most per record for each data breach ($201 per record) followed by Germany ($195 per record). The total cost for data breaches amounted to around $300 million in 2013.[[42]](#footnote-43)

* **Contribution**: The smart grid critical infrastructure is a target of different cyber attacks therefore the consortium will demonstrate SecureCloud platform will improve the credibility of the computing technique for Smart Grid applications.

The consortium will develop the appropriate use cases for demonstration of SecureCloud’s platform capabilities to improve the competitive position of the European and Brazilian cloud sector on example of smart grid critical infrastructure.

* **Contribution**: The consortium will implement a validation process based on a dedicated environment supported by the Israel Electrical Corporation. This environment allows to develop and to test tools and methodologies over mirrored critical infrastructures, assessing risk and simulating real scenarios.

IEC will customize its validation environment for specific requirements of SecureCloud project. The project partners will use the environment for system development and integration, and for validation cyber attacks.

* **Contribution**: The consortium will develop and validate a platform for smart metering applications focusing on the security requirements necessary for smart metering sector of Brazilian energy sector.

SecureCloud platform will be created and validated to enable both the storage of critical data and specific software for smart metering and fraud detection systems, according to the requirements used by Brazilian utilities. All those solutions will be validated using real smart metering data acquired by Lactec on its Smart Grid pilot and in Brazilian utilities systems.

**Expected impact**: *Facilitate the development of cloud enabled applications through robust standardized global technologies.*

* **Contribution**: Design and implement services that manage secure containers in an open-source middleware.

Using a service-oriented approach, we will provide generic services that build a foundation for implementing cloud-based platforms for secure applications. Using these services, secure resources will be managed at the same level of abstraction as typical cloud infrastructure resources, such as object storage, VMs and volumes. This will enable cloud providers to use secure resources efficiently and cloud customers to build cost-effective secure applications.

* **Contribution**: Identify and propose patterns for cloud-based big data applications that are quality-of-service, privacy, and security aware.

The SecureCloud project will develop a rich set of applications that combine security, privacy and QoS at different levels. Our diverse and experienced partnership will ensure that these applications are effective and practical. It can thus identify patterns and offer templates for the implementation of other applications that should observe security, privacy and QoS, even in other domains.

* **Contribution**: Data privacy in cloud services has been a matter of debate in recent years. There is a lack of trust in cloud providers since they are able to read personal data (as stated in various Terms of Service), share it with governmental agencies, or be breached by malicious attackers. In SecureCloud, we will address the problem of data privacy by using cutting-edge technology allowing us to store data with different levels of protection and in multiple locations.

SecureCloud will allow cloud developers to manage data privacy of stored data by design and using different levels of security for the data, including the distribution of data amongst multiple cloud providers. These capabilities can be integrated seamlessly with standard technologies for communicating with existing Cloud providers. These strategies and capabilities are key due to (i) the increasing legal constraints for storing data within the borders of EU countries, and (ii) the fact that European countries have been found to receive four times more cyber attacks than the US.[[43]](#footnote-44)

* **Contribution**: SecureCloud will develop a validation system for demonstration and evaluation of cloud-based services in federated, heterogeneous and multi-layered cloud environments, of the dynamic provisioning of interoperable applications and services, as well as technologies integrating cloud and big data in terms of architecture, middleware and services, applied to a smart metering application.

The validation as developed in SecureCloud will establish a new level of secure technology for the cloud and will demonstrate how this technology can be adapted for faster adoption by critical applications similar to those of the smart grid.

**Expected impact*:*** *Joint contributions to International Standardisation and/or Forum activities*

* **Contribution:** The project will closely monitor the main standards and/or standardization activities that are relevant for cloud computing security. The work of the main standardization bodies, technical committees, and forums will be followed closely, to ensure that results be used in SecureCloud.

The indications provided by the by the selected standardization bodies, technical committees, and forums will be promoted via the participants’ network of connections, to form a triple-helix collaboration commitment among leading companies, research centres, and universities and to cluster with relevant funded projects in Europe, in alignment with the aims of Horizon 2020.

* **Contribution:** Some of the partners of the consortium have been active contributors for several years to standardization bodies that are of specific interest to the project.

Members of SyncLab are actively involved in and willing to contribute to ETSI TISPAN WG6 and some IETF Working Groups, as well as ETSI Cloud Technical Committee and IETF initiatives on cloud computing standardization.

### Alignment with EU strategies and policies

SecureCloud is perfectly aligned with EU strategies and policies on cloud computing security, and in particular with the Digital Agenda for Europe (DAE), successor of the i2010 initiative, which is one of the main strategy pillars for building a thriving digital economy by 2020. Security is one of DAE main focuses, and it is tackled by several actions. Specifically, SecureCloud will contribute to the following Digital Agenda actions:

* Action 28: Reinforced Network and Information Security Policy
* Action 29: Combat cyber-attacks against information systems
* Action 32: Strengthen the fight against cybercrime at international level
* Action 33: Support EU-wide cyber-security preparedness

In 2012, Commissioner Neelie Kroes announced her “plan to launch a Cloud Computing Strategy that would make Europe not only cloud-friendly but also cloud-active.” The European Cloud Partnership (ECP), and overall cloud computing strategy, is expected to be defined and developed with a special emphasis on cyber security in cloud environments. It is also envisaged that the European Commission will proceed with the legislative process towards adopting the “Directive on Attacks against Information Systems” at a European level. A proposal was put forward in September 2010, superseding and supplementing the decision by the European Union Council from 2005, taking also new developments into account. Member States are required to adopt this Directive within two years from the general implementation. Similarly, the European Commission is currently in the process of reviewing the general EU data protection act legal framework. The outcome should result in more legal certainty through clearer definitions and greater harmonization. European Strategy for Internet Security is also being currently developed and has specific objectives to foster close co-operation and early warning between Member States competent authorities, and between competent authorities and the private sector, by ensuring adequate capacities, prevention, detection, mitigation and response at national and EU level.

The novel dependability enhancing techniques and COTS-based solutions that will be delivered by the SecureCloud project contribute precisely to the achievement of the objectives set by the DAE and the European Cloud Computing Strategy.

As to the main reference application domain of the project, namely Critical Infrastructures, the SecureCloud research plan is perfectly aligned to the measures taken by the EC aimed at improving the protection of critical infrastructure in Europe, across EU States and in the most relevant sectors of the economic activity, and notably the European Programme for Critical Infrastructure Protection (EPCIP), launched by the European Commission to reduce the vulnerabilities of critical infrastructures, and to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures.

### Assumptions and external factors

Factors that can limit the expected impact of a technology-oriented project are largely non-technical. Many sectors of industry are reluctant to adopt new approaches/technologies, even if there is tangible evidence that they have superior characteristics. In some cases, this hesitation can be justified (e.g., if safety is an issue, the new technology has to be well proven before it can replace existing solutions). This is exactly the case of the business domain targeted by the project. The consortium is well aware of the necessity of providing convincing evidence of the effectiveness of the solutions that will be developed by the project. Hence, the decision of developing substantial use cases, and to perform a thorough validation and demonstration campaign. In other cases, the only explanation for being reluctant to adopt new approaches is no more than inherent conservatism. Security-enhancing features (such as those that will be developed by SecureCloud) are unarguably commercially-relevant solutions and the SecureCloud consortium has all the skills that are needed to deliver technically sound solutions, but assuming that these factors alone are sufficient to guarantee acceptance of the project is naive, and may ultimately result in partial or even total failure of the project to achieve impact. Awareness is very much needed that there can be factors outside the control of the project that can impede the take-up of project solutions. SecureCloud partners do have this awareness, and they have thus taken effective measures to ensure that these external factors be transformed into factors that are under the control of the project.

The most important measure that the SecureCloud consortium has taken is the design constraint of making SecureCloud solutions available to applications via a widely accepted interface, namely the Open Stack API. What sets SecureCloud apart from most other cloud projects is that SecureCloud does not aim at developing yet another cloud platform, rather it aims at providing flexible mechanisms and controls that can be implemented and enforced on top of existing Commercial Off The Shelf (COTS) cloud solutions (specifically, those compliant to Open Stack), running on commodity hardware. Since SecureCloud security-enhancing features are provided via an interface that gathers wide consensus, this design choice guarantees all the conditions that can help maximize the impact of SecureCloud outputs in the real world.

The design and the implementation of an integrated solution becomes much more complicated as compared to an unconstrained project recreating the cloud environment. In SecureCloud, we decided to trade-off design simplicity for project impact. The important advantage of this approach (and the reason why we accepted to take the additional burden of more complex design and implementation) is that by doing so, we have mitigated (if not eliminated) the dependence on external factors of project potential (in terms of impact). The possibility of achieving impact has been transformed into the ability of designing and implementing the mechanisms that we have promised. We claim that the SecureCloud consortium assembles all the skills (both technical and managerial) that are needed to guarantee that such promises will be delivered.

Also importantly, an additional measure that has been taken to maximize SecureCloud impact was involving partners—both industries and use case providers—who are already engaged in the business sectors where the project expects to make an impact.

## Measures to maximise impact

SecureCloud has identified a number of measures that will be taken to ensure that its results have the impacts described above. The reason why a multitude of diverse actions has been planned is the awareness that technical innovativeness is the foundation for impact, but it is not sufficient alone to guarantee that impact will actually be achieved. In this section, we first discuss the measures that project will take to achieve impacts.

A first important avenue to achieve impact that sets SecureCloud apart is the decision to give substantial emphasis to demonstration of project solutions. Realistic demonstrators, i.e., that either operates under real conditions or closely mimic them, will be set up for each use case. Not only will this allow us to showcase project results with respect to the business domain that we target—namely: Critical Infrastructures, and particularly the smart grids—but (most importantly) **it will qualify SecureCloud technology for TRL6**.

A second important avenue to achieve impact that sets SecureCloud apart is the composition of the Advisory Board (described in detail in section 3.2.1), that includes several categories of stakeholders: large companies (Intel and SAP), a university (KTH, Sweden), and a city hall (Curitiba, Brazil). Such a prestigious and multi-faceted AB is not usually seen in research projects.

Another measure for achieving impact will of course be the dissemination activities that will ensure the proper impact within the scientific community. SecureCloud consortium targets top conferences with very high visibility both within and outside Europe. Dissemination activities will be led by Sync Lab and will be reported in periodic deliverable D6.3.

Yet another measure for achieving impact will be communication activities, described in detail in a separate sub-section below. All members of the consortium will participate in the communication activities. Moreover, a periodic research newsletter will be created and managed by Sync Lab (deliverable D6.6).

Sync Lab will be in charge of creating and maintaining a constantly updated public website (deliverable D6.1) which will ensure further uptake of SecureCloud results. The Website will be reachable on a specific domain name for the project, and will be registered and kept alive for at least three years beyond the project end. It will be simple and will be always up to date and accurate, with respect to both contents and news. The website will target European and Brazilian audiences, but may also generate interest to a broader audience. It will acknowledge EU, Brazilian and Swiss funding, use the EU and national flags when appropriate, but avoiding contract jargon. It will include a project logo designed by a professional and provide interoperable RSS feeds support/services.

Another important measure for achieving impact will be collaboration activities. While detailed planning of collaboration activities is not possible at proposal submission time (since too many variables are yet unknown), we explicitly state our commitment to actively participate in any relevant initiative promoted by the EC for favouring synergies among projects in the same objective and/or in related objectives.

SecureCloud results will also contribute to open source offerings, and thus ensure for the SecureCloud impact in the developer community.

### Standardization

Many Standards Development Organization (SDOs) are currently working on cloud computing whitepapers, standards, and specifications. Here is a non-exhaustive list of such SDOs:

* NIST National Institute of Standards and Technology. The goal of NIST is to promote the effective and secure use of the cloud computing technology within government and industry by producing technical guidelines and standards. A first recommendation published in September 2011 provides the NIST definition of Cloud Computing.[[44]](#footnote-45) The NIST definition characterizes important aspects of cloud computing and is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing. Another relevant recommendation is the Special Publication 500-292 that presents the NIST Cloud Computing Reference Architecture.[[45]](#footnote-46) In this recommendation security and privacy concerns as well as security responsibilities for different cloud service models and deployment models are discussed. NIST also produced the Cloud Computing Synopsis and Recommendations document[[46]](#footnote-47) that addresses system integrity and data privacy issues, and analyses the risks of unintended data disclosure in clod environments.
* ISO/IEC JTC1 SC38. The Study Group on Cloud Computing (SGCC) has been created to investigate market requirements for standardization, initiate dialogues with relevant SDOs and consortia, identify challenges to be addressed, and provide a taxonomy, terminology and value proposition for Cloud Computing.
* Global Inter-Cloud Technology Forum (GICTF). This forum aim to promote standardization of network protocols and the interfaces through which cloud systems interwork with each other, and to enable the provision of more reliable cloud services than those available today. Two documents have been released by the GICTF, the first one is a white paper on technical requirements for supporting the intercloud networking,[[47]](#footnote-48) while the second one is the intercloud interface specification.[[48]](#footnote-49)
* ETSI Cloud Technical Committee (TC). This Technical Committee focuses on interoperable applications and services based on global standards and the validation tools to support these standards.
* Distributed Management Task Force (DMTF). DMTF's Cloud Management Initiative is focused on developing interoperable cloud infrastructure management standards and promoting adoption of those standards in the industry.
* CSA Cloud Security Alliance. The mission of CSA is to promote the use of best practices for providing security assurance within Cloud Computing. Two Working Groups have been established to deal with cloud computing security issues, namely the Cloud Vulnerabilities Working Group and the Cloud Data Governance Working Group. The Cloud Vulnerabilities Working Group is global working group chartered to conduct research in the area of cloud computing vulnerabilities, with the goals of understanding and educating the classification and exact causes of cloud computing vulnerabilities, recommendations and best practices for the reduction of top vulnerabilities, reporting of vulnerabilities and the development of related tools and standards.
* The Cloud Data Governance Working Group focuses on the analysis and specification of requirements and needs of different stakeholders on governing and operating data in the Cloud.
* Telecommunications Management Forum (TMF). TMF is currently working on the cloud services management to cover Cloud Business Process Framework and Cloud Service Definitions.
* Open Grid Forum (OGF). The purpose of the Open Cloud Computing Interface working group (OCCI-WG) of the OGF is the creation of a practical solution to interface with Cloud infrastructures exposed as a service (IaaS). OCCI-WG focuses on a solution which covers the provisioning, monitoring and definition of Cloud Infrastructure services.
* Storage Networking Industry Association (SNIA). SNIA produced the Cloud Data Management Interface (CDMI) standard. The Cloud Data Management Interface defines the functional interface that applications will use to create, retrieve, update and delete data elements from the Cloud.
* OASIS: Identity in the Cloud Technical Committee. The OASIS IDCloud (Identity in the Cloud) TC works to address the serious security challenges posed by identity management in cloud computing and gaps in existing standards. The purpose of the TC is to harmonize definitions, terminologies and vocabulary of Identity in the context of Cloud Computing; to identify and define use cases and profiles; and to identify gaps in existing Identity Management standards as they apply in the cloud.
* Alliance for Telecommunications Industry Standardization (ATIS). ATIS created the Cloud Services Forum (CSF) that promotes the integration of cloud technologies and network infrastructure to realize the significant benefits of cloud, by developing standards to enable the network to do more than it does today (e.g., expanding product offerings including services on demand, accelerating time-to-market, lowering costs, minimizing complexity, increasing scalability), focusing on the creation of reusable Service Enablers to progress each phase of work; and creating technical solutions in support of a global marketplace to help Service Providers realize cloud’s full potential.
* IEEE. IEEE started two working groups on cloud portability and Intercloud interoperability. Standardization areas of the Cloud Profiles Working Group (CPWG) include application interfaces, portability interfaces, management interfaces, interoperability interfaces, file formats, and operation conventions, while the Intercloud Working Group (ICWG) is working to the standard definition of topology, functions, and governance for cloud-to-cloud interoperability and federation.
* Open Data Center Alliance (ODCA). This Alliance has delivered the first customer requirements for cloud computing documented in eight Open Data Center Usage Models which identify member prioritized requirements to resolve the most pressing challenges facing cloud adoption.
* The Open Group Cloud Computing Work Group. The goal of the Open Group Cloud Work Group is to create a common understanding among buyers and suppliers of how enterprises of all sizes and scales of operation can include Cloud Computing technology in a safe and secure way in their architectures to realize its significant cost, scalability and agility benefits.
* ITU-T Focus Group on Cloud Computing (FG Cloud). ITU-T FG Cloud is structured in two Working Groups, namely WG1 and WG2. Standardization efforts of WG1 are focused on cloud definition and taxonomy, cloud security, infrastructure and network enabled cloud, cloud services and resource management, while activities of WG2 include gap analysis and action plan for development of relevant ITU-T cloud standard.

Participants to SecureCloud have already contributed to standardization activities on network security and information management. The project will explore the possibility of contributing to existing standards, for example by providing comments on working documents being circulated during the project life-time. In case the SecureCloud project gets funded, the project partners intend to exploit the results achieved in the project to contribute to the SDOs working in the field of Cloud Security.

### Dissemination and exploitation of results

Dissemination and preparation of exploitation of the project results are issues addressed within WP6. Dissemination activity is considered any task that aims at disseminating the results of the project, promoting the SecureCloud concept, increasing the visibility of the project and supporting the exploitation of the results achieved. Dissemination and exploitation measures that the Consortium has planned address the full range of potential users and uses. The approach to innovation is comprehensive, and it is tailored to the specific technical, market and organisational issues addressed by the project. In order to achieve these goals, massive dissemination and exploitation activities have been planned, that will span the entire duration of the project. For better performance, activities will be organized in several subtasks, and in particular: Raising User Participation and Awareness; Web-based dissemination and Social networks (e.g. Facebook, Twitter, Vimeo, YouTube); Printed dissemination material; Workshops and Conferences; Publications; Radio interviews; Exploitation planning; Clustering with other projects; Market analysis; Exploitation plan; Coaching; Training and knowledge transfer; Production of training material; Organization of training events.

SecureCloud’s dissemination activities can be summarized as follows:

* Archiving SecureCloud reports, deliverables and data to open access portals: Special emphasis is given in fostering the open access of the SecureCloud results on the SecureCloud website;
* Exploitation of 2 workshops to foster the interconnection with the industrial and end-user needs analysed in the following paragraphs;
* Participation in exhibitions/forums to promote the exploitation of the SecureCloud results;
* Social media through the creation of special groups that inform interested users about the current research achievements of SecureCloud and events that are interested in the project.

SecureCloud’s consortium plans to organize two international events on Cloud security, data mobility and confidentiality and integrity of cloud infrastructures. With cloud being the trend that affects different sectors, it is important to organize venues with the main actors will be involved. The proposed events will have two main objectives:

* On one hand, the SecureCloud project dissemination and presentation of its results.
* On the other hand, to generate awareness about the cloud security impacts on the economy and get a consensus about the technologies, procedures.

To this extent, experts from different sectors will be invited, as well as existing networks on Cloud security, and representatives of other projects approved under the Cloud call. The European Commission and other public institutions will be also invited to play different roles as speakers and moderators.

The first event is foreseen to be organized in the first year of the project, during two days. The second event will be the SecureCloud’s final event, so it could for instance be organized in Brussels at the end of the project and it last for one day. The aim of this final event is to highlight and give visibility to the project’s results as well as disseminate them to a broader audience. The speakers, other than the project’s partners, would be European Commission representatives, other cloud projects, industry representatives, international networks as well as other interested stakeholders.

SecureCloud has identified other relevant forums and international conferences that represent significant dissemination vectors. The dissemination strategy of SecureCloud foresees participation of representatives from the consortium and sponsorship of events on Cloud. An indicative list of such events that the consortium will attend in order to promote the findings and advances of the project include:

* Cloud Expo - http://www.cloudexpoeurope.com/
* ETP4HPC, the European Technology Platform for High Performance Computing (HPC)- http://www.etp4hpc.eu/
* Data Centre World - http://www.datacentreworld.com/
* Cloud Open Europe - http://events.linuxfoundation.org/events/cloudopen-europe

The SecureCloud Dissemination and exploitation Strategy will provide clear and objective action plan for effective and efficient dissemination and awareness about the project’s objective and results. This strategy will be implemented through the Awareness and Dissemination Plan which will be prepared and deployed along the project and beyond. The plan will be based on:

* A detailed identification of the target audience and stakeholders and of the partner’s contacts and networks.
* The different types of dissemination and communication material/instruments/means that will be used during the project and afterwards.

By disseminating the project aims and results, SecureCloud will ensure:

* Knowledge transfers and exchange not only between partners but also with other European projects and entities working in the same field, creating a network of exchange and mutual learning;
* Encourage new developments and research in the field of Cloud security;
* Transfer the acquired knowledge to different sectors especially focusing on the use case domains in order to improve the competitiveness of the European industry.

One of the objectives of the Dissemination Plan is to draw attention of national governments, regional authorities, public and private organizations, and citizens to the needs and benefits of the project, generating thus a market demand for the results of SecureCloud.

The following dissemination tools will be used in order to enhance the reputation and visibility of the project and the consortium: the Web, apps, regular media, events, publications, social networks and international events.

### Training

The academic partners already offer—also in cooperation with other outstanding European universities—Masters and PhD school programs that are closely related to the research that will be done in SecureCloud, e.g. the International Master's Program in Distributed Systems Engineering (TUD). In case of funding, a PhD school will be jointly organized by the academic partners, featuring and industry session by the industrial partners of the SecureCloud project.

Also importantly, SecureCloud academic partners are actively involved in a number of technology transfer programs, aiming at favouring early adoption of emerging technologies by the local industry. In case of funding, SecureCloud results will be included in initiatives to which they will participate.

### Initial dissemination plans

TUD, as the coordinator of SecureCloud, will ensure all the activities aiming at maximizing projects impact to the research and industrial community. This will be accomplished by exploiting the existing communication channels in domains relevant to the scope of SecureCloud. TUD will promote SecureCloud’s outcome in the following ways:

1. Promoting SecureCloud’s website.
2. Liaison with other cloud computing projects within the scope of H2020, especially those in which project partners are directly or indirectly involved into. This will provide swift and efficient interactions for fruitful information interchange, and cooperation on common ideas that could serve for multiple projects.
3. Attendance to events, workshops, and exhibitions along the course of the project. In particular, SecureCloud partners aim at participating in exhibitions and conferences organized by the Cloud Security Alliance, ENISA, ISACA and NIST, in order to create public awareness. To this ground the project has defined a dissemination strategy that includes involvement in working groups of the aforementioned associations.
4. A direct communication channel with ENISA will be searched, in order to have a two-fold communication of the project’s results.

Universities:Academic partners are interested in keeping their track record deriving from the publication of at least ten conference papers per year of the project, as well as from six to eight journal papers within the entire project’s lifetime. Among conferences, the targets will be partly represented by the most well-known forums in the field of security and dependability (SIGCOMM, DSN, SRDS, etc.). Coming to the journals, partners aim at contributing to magazines like IEEE Transactions on Dependable and Secure Computing and IEEE Security and Privacy. They will disseminate scientific results of the project in the form of publications, conference presentations and posters, lectures and tutorials. They will aim at top-tier peer-reviewed conferences in the fields of distributed systems (EuroSys, PODC), dependable systems (DSN, SRDS), security and privacy (USENIX Security Symposium), networks and communications (SIGCOMM), cloud computing (CCGrid, CloudCom). The priority will be given to the high-visibility conferences and journals with an acceptance rate of at most 20%. After the end of the project, they will ensure further dissemination of the gathered knowledge not subject to legitimate interests.

General software industry and SMEs:Industrial partners plan to disseminate SecureCloud results both externally and internally, by means of multiple dissemination channels to communicate to their customers and other stakeholders about the advantages of integrating security-enhancing mechanisms in their cloud platforms and cloud-based applications. They will also target dissemination activities towards policy-making stakeholders at the national level.

SecureCloud will mention the EU’s subsidy in all promotional material, and will feed back to the EC by means of a set of success stories that will show the project’s positive progress. The work from SecureCloud will be used to contribute to the on-going development of national and international security codes of practice and standards for utility networks, through liaison with EU and national authorities.

### Expected exploitable results

Usage of cloud offerings independently of the deployment and the service model is proven a very profitable investment for SMEs and large companies with multiple benefits regarding ROI (Return on Investment), since the deployment cost for the service is reduced. Main concerns are associated with the data migration and user mobility and how the confidentiality and privacy is preserved.

In order to ensure maximal exploitation of project’s results SecureCloud has adopted a stepwise approach:

* Step 1: Technology review update (not SOTA analysis) of all relevant background including cloud security as well as technologies and techniques for fault and intrusion detection, auditing facilities and secure communication channels taking into account international and national directives and European strategies in order to carry out complementary primary research where required.
* Step 2: Analysis of complementary and competitive services and relevant shortcomings that need urgently to be addressed at a global level in order to pave the way of cloud adoption by industry, as well as identification of emerging best practice across several domains that addressed by the project and involving huge data processing as well as the wider involved public and private domain internationally.
* Step 3: Setting up of deployment scenarios, market and business models for individual exploitation and joint exploitation, specifying collaboration roles, costs and revenue flows, specifying as well necessary guidelines that need to apply in order to make such scenarios feasible;
* Step 4: Validation of business models and deployment scenarios within the feasibility analysis with the help of the partners’ complementary expertise and assessment of the effectiveness of the SecureCloud approach to provide a leap forward in the area of cloud security in different domains.
* Step 5: Organization, planning and execution of wide impact dissemination activities to create full awareness of SecureCloud activities, its approach and results in the academic community, among public authorities, service and solution providers as well as contributing to the EU strategic roadmap for the fast adoption and usage of cloud security modules; establishing contact with key third parties for exploitation.
* Step 6: Regular review, revision and refinement of partner-specific exploitation plans and joint and collaborative business plans in the light of interim project results; formalization of service level and other appropriate agreements for joint exploitation among partners and third parties;

The SecureCloud consortium under the auspices of the coordinator and with joint exploitation activities organized and coordinated by Sync Lab aims at promoting novel solutions and products in several market places and segments such as Healthcare, telecommunication, gaming and authoring, public protection, security and the banking sector.

### Preliminary exploitation plans

Universities: SecureCloud Academic partners value the principle of cross-fertilization between academia and industry, since it brings together the complementary expertise and vision of the variegated group of university researchers and industry professionals that build up the consortium. The practice of close cooperation between the academic and the industrial communities that is an intrinsic characteristic of SecureCloud Academic partners will provide a major avenue for market exploitation of SecureCloud solutions. Also importantly, SecureCloud Academic partners’ brilliant track records in key fields like network security and resilience, intrusion detection, cloud security, and system dependability paves the way to successful exploitation of the project outcomes in the form of advanced research consultancy activities to industries that are engaged in the design and development of cutting-edge technologies and applications for secure cloud computing environments. The exploitation activities sketched above will be promoted and supported by organizing dedicated initiatives and/or events aiming at creating opportunities for commercial dissemination of project results to the industries and public administrations, as well as to the public in general. Exploitation activities will be performed in collaboration with all SecureCloud partners.

Industry and SMEs: All industry partners’ expertise in the area of security in cloud platforms will increase due to international collaboration with major players and academic partners, and they will achieve competitive advantages to reinforce their presence in national and international markets, and enter new markets as well.

CloudSigma is a global company with an ambition to expand its presence in Europe and Brazil, among other markets. By participating in the SecureCloud project it expects to gain deeper insight into the cloud resource requirements and to attract new customers to its platform. As a commercial cloud provider, it is extremely beneficial to CloudSigma to gain knowledge of the potential market segments. Besides, its involvement in SecureCloud will allow it to be better positioned to understand the requirements and expectations customers have with regard to security. Unless when agreed otherwise by the Consortium, any extensions to CloudSigma’s API developed during the project will be documented and made publicly available to its client base.

Lactec has been developing research and development projects for smart metering and other smart grid applications for several utilities in Brazil, focusing more in the development of hardware and embedded systems, including security. CAS technology is the main integrator of metering systems for Brazilian market, providing metering data management systems for the majority of utilities in the country and Copel is the utility that delivers energy for the state of Paraná in Brazil, which covers more than 300 cities and 2 million consumers. Lactec, CAS and Copel have worked together in several research and development projects, including one pilot of Smart Grids, located in Curitiba. All these companies will be directly affected by the results of SecureCloud, as well the whole energy sector in Brazil.

ChocolateCloud is a cloud service provider that offers efficient and flexible cloud technology solutions, exploiting the power of network coding for delivering high performance and reliability to its customers. SecureCloud will allow ChocolateCloud to take its current Secure Any Cloud solutions to a higher technology readiness level, as well as developing, testing, and deploying critical and flexible data privacy. This will provide an additional product and set of features to its current product offering.

### Management of knowledge and intellectual property

In accordance with the H2020 rules for participation, the consortium agreement will govern dissemination, access rights and use of knowledge and intellectual property. In order to make sure that these terms are followed, to avoid disputes and to facilitate business planning, the Management Board will maintain an IPR Directory throughout the lifetime of the project. This document will list all items of knowledge relating to the work of the project (both pre-existing know-how and results developed in the project), and make explicit for each item:

* The owner(s).
* The nature of the knowledge, and its perceived potential for exploitation.
* The currently agreed status of the item concerning access rights, plans to use the knowledge in exploitation, or plans to disseminate it outside the consortium.
* Measures required, or in place, to ensure protection of IPR for the item.
* The directory will be regularly updated, and available to all partners. It will form a key tool to enable knowledge management.

To maximise societal impact, the project will disseminate some knowledge outside the consortium. An initial version of the IPR directory will be created at the start of the project. The project coordinator is responsible for the use of IPR within the consortium, according to the terms laid out in the Consortium Agreement. In general, tools, methodology documents, benchmarks and case studies will be available to all; while some proprietary tools and algorithms developed by the partners may be available at the discretion and terms of their respective owners. In spite of the latter restriction, all the partners intend to pursue publications of the underlying principles of the technologies embodied in their tools in the appropriate academic conferences and industrial events/user groups. Finally, all knowledge will be managed in accordance with the Grant Agreement and a consortium agreement that will be timely prepared and signed by all consortium members.

### Research data management plan

##### Policy for Data Management

SECURECLOUD plans to participate in the Open Research Data Pilot. To cover that aspect a Data Management Plan (DMP) is periodically issued, to detail what data the project will generate, whether and how it will be exploited or made accessible for verification and re-use, and how it will be curated and preserved. A first version of the DMP will be provided at the sixth month of the project (D6.2), and two updates are planned at month 24 and 36. Furthermore, if necessary, additional releases of this deliverable will be provided. The consortium plans to deposit data in a research data repository, and will take measures to enable third parties to access, mine, exploit, reproduce, and disseminate the data free of charge.

##### How data will be exploited and/or shared/made accessible for verification and re-use

The data will be shared after proper processing, aiming at removing any information that could be mapped to the identity of real people, via accurate (pseudo-) anonymisation techniques. Anonymised data will be made available via multiple channels, and in particular: 1) it will be posted on the project Web site, in an area that will be accessible to the followers of the SECURECLOUD project; 2) it will be shipped on digital support upon request (and compilation of a form); 3) it will be deposited in a research data repository, from which external users will be given the possibility to access, mine, exploit, reproduce and disseminate it free of charge; 4) it will be shared within the context of possible future initiatives promoted by the EC. Some of the data is governed by a very stringent and cumbersome set of legal requirements that restricts its use for research. However, anonymised data that demonstrate the use of the system can be made available given that all legal requirements are fulfilled.

##### How will data be curated and preserved

The data will be curated with respect to the relevant legislation, securing sensitive information and preventing private’s data eavesdropping. For each use case the corresponding provider will store the original data locally at their respective premises. Data curation will include augmenting the data with associated metadata, for specifying the semantics. Data preservation will be ensured by having the Coordinator and the Technical Coordinator each store a copy of the original data at their respective premises, on a RAID device. The data will be stored, archived, and preserved for the duration set by the legal framework.

### Communication activities

The consortium has great confidence in its ability to produce high quality deliverables and disseminate the project findings based on their considerable past experiences, as shown by the further information listed in partner profiles enclosed in the proposal. More complete lists of the consortium’s related experiences and publications can be found on the websites of the individual partners. Furthermore, several of the partners have participated in previous EU funded projects, exhibiting high involvement in communication initiatives.

Communication covers all actions by which the activities, knowledge, results and ideas generated in the project are shared with the relevant stakeholders. Communication requires that all ideas that can be communicated in an open arena will be made freely available. In this case, we will ensure the widespread dissemination of public results of the project to the stakeholders in the EU Member States and the Associated Countries.

For the communication activities, the SecureCloud consortium will perform a set of actions that will ensure efficient dissemination of the project’s activities and results at a European dimension. The project foresees to implement a very concrete communication strategy that will evolve towards the overall enhancement of SecureCloud’s project impact in a measurable way aligned with the technical progress of SecureCloud.

The modules that will strengthen consortium’s vision will include:

1. The definition of the key messages directly connected with the expected results.
2. The identification of target group audiences based on specific criteria and classified according to different categories, such as: Research community; Large industries; SME; IT security; Network security; IT product providers.
3. Selection of modes of communication in order to use the available channels both proactively and reactively. This will include the following:
   * Creation of a mailing list and of dedicated social network accounts for pushing dissemination related information and attracting attention. The mailing list will be developed by utilizing the affiliations and memberships of the consortium members, as well as additional groups and networks of contacts.
   * Project story – factsheet: SecureCloud will prepare shortly after the project start a project factsheet, which will be made available to the EC for publishing in EC communication initiatives/facilities, collected in printed publications together with related projects’ factsheets, and any other suitable opportunity.
   * E-mails/newsletters to specialized stakeholders such as associations and companies working with cloud in order to maximize raising awareness to the project and/or the latest news in it.
   * Press releases/articles that will be professionally written, reporting about the more recent developments and/or results of the SecureCloud project will be published in both the SecureCloud’s web site and the media. These press releases will be sent to European Commission, national, local and sectorial means, like journals and newsletters for publishing news.
   * Interviews - At local radios, TVs, and printed press aside to field specific and international communities, also local communities will be targeted, also in local languages, by dissemination activities.
   * Exploitation of the consortium partner’s institutional/company websites for disseminating news and providing links to the project official website.
   * Events that will be organized by the SecureCloud consortium targeting specialized stakeholders such cloud providers, SMEs, security associations as well as the public at large, in order to illustrate the benefits that are brought about by the project. As a measurable outcome the consortium foresees the organization of two major workshops in order to communicate the project findings.
   * Meetings with local Member European Parliament (MEP) representatives, to raise the MEP's awareness of the impact EU Framework funds are having locally.

The success of this dissemination plan and communication strategy will be measured by the following:

1. Feedback and comments received as a result of posting project information and respective activities that are being developed on the project website.
2. Responses to e-mails directed to various stakeholder groups to which a copy of report(s) and/or an executive summary will be attached.
3. Number of stakeholders interested to become aware of the SecureCloud project outcomes.
4. Comments and views provided by participants at workshops and seminars.
5. Detailed website access statistics produced on a regular basis.

A fairly high number of conferences and events related to Cloud Computing Security have recently taken place. This is a clear evidence of the interest in the research topics that SecureCloud intends to address. Therefore the consortium partners have already started to select future conferences, workshops, and events in the domains of cloud computing security and dependable distributed systems, where the results of the SecureCloud project will be presented and disseminated, and the achievements and plans of the consortium will be discussed and coordinated with related initiatives. The consortium will for every publication not only choose the conference and the journal based on its reputation and quality but also based on the kind of open access options that they provide, in accordance with the guidelines on Open Access to Scientific Publications and Research Data in H2020. Primary choice and focus will thereby be the open access gold path. However, this might not always be the best way to disseminate the project results, as not all top-tier conferences and journals offer such an option. In these cases, we target at least green open access, as supported for example by ACM, IEEE, and the USENIX association (that host many of the top tier conferences in the computer science area). In case of green open access we will utilise Qucosa (http://www.qucosa.de), an offering by TU Dresden, or an equivalent facility.

The contributions to the project will be presented in priority in conferences and journals that have a high visibility and a low acceptance rate. There publications will be completed by external talks and tutorials by the researcher of the project. In particular, we target the following conferences and journals (but are not limited to):

* Distributed systems design and implementation: Systems Design and Implementation (NSDI), Symposium on Operating Systems Principles (SOSP), Operating Systems Design and Implementation (OSDI), International Conference on Distributed Computing Systems (ICDCS), ACM Transactions on Computer Systems (TOCS), Computer Networks (ComNet), IEEE Transactions on Parallel and Distributed Systems (TPDS), Annual International Conference on Computer Communications (INFOCOM),
* Dependable systems: Dependable Systems and Networks (DSN), Symposium on Reliable Distributed Systems (SRDS), IEEE Transactions on Software Engineering (TSE),
* Data processing and extraction: World Wide Web conference (WWW), ACM SIGCOMM conference,
* Data storage: USENIX Conference on File and Storage technologies (FAST), EuroSys conference,
* Performance, scalability, networking aspects: IEEE International Symposium on High Performance Distributed Computing (HPDC), ACM SIGCOMM Conference, IEEE/ACM Transactions on Networking (TON),
* Security: Internet Society's Network and Distributed System Security, ACM Conference on Computer and Communications Security (CCS), IEEE Security and Privacy, RSA conference, Applied Cryptography and Network Security (ACNS), European Symposium on Research in Computer Security (ESORICS), IEEE International Conference on Trust, Security and Privacy in Computing and Communication (TRUST), International Conference on Information Security and Cryptology (ICISC);
* Evaluations and demonstrations: International Conference on Cooperative Information Systems (CoopIS), International Conference on Objects, Models, Components and Patterns (TOOLS), Symposium On Applied Computing (ACM SAC).

# Implementation

## Work plan — Work packages, deliverables and milestones

### Overall strategy of the work plan

The overall objective of the SecureCloud project is to:

1. develop a secure Cloud platform based on secure containers enabling the development of secure applications which follow the Micro-service architecture paradigm
2. evaluate the SecureCloud platform using two big data related smart grid use-cases:
3. privacy-preserving processing of smart meter data
4. QoS-guaranteeing smart grid technologies

In order to achieve these goals the overall work plan is divide into seven work packages—five technical and two non-technical ones (cf. Figure 3.1-1).



Figure 3.1‑1: Work packages of the SecureCloud project

The two non-technical work packages are dedicated to the overall project management (WP7) and the dissemination, exploitation and communication of the project result. Consequently WP7 is led by the coordinator TUD and WP6 is led by the Exploitation and Innovation Manager (EMI) SYNC. Within WP6 market analyses and business plan development will be executed together with an exploitation plan in order to prepare, support, and present business initiatives and opportunities created by the project. Moreover WP6 will organise the contributions to standardisation of the SecureCloud project.

The five technical work packages can be further divide into three groups:

* Application: WP5 which is dedicated to the development and evaluation of the two mentioned demonstrators
* Components: WP2, WP3 and WP4 which will develop the actual components which form the SecureCloud platform
* Platform: WP1 which collects the requirements, develops the overall architecture and manages the AGILE development cycle.

WP5 Demonstration and Evaluation is dedicated to the development and evaluation of the two mentioned demonstrators. As the demonstrators use the SecureCloud platform, developing and evaluating the demonstrators will indirectly evaluate the SecureCloud platform. This holds on the one hand for the security features offered by the SecureCLoud platform, i.e. if these features are sufficient to implement a privacy-preserving Smart Meter data processing where neither the cloud provider nor the utility will learn any personal data. On the other hand it holds as well for the QoS-guaranteeing Smart Grid use case, as the achieved QoS of the envisaged fault detection and recovery mechanisms heavily depend on the compliance of the underlying SecureCloud platform to their QoS guarantees. Moreover WP5 contributes use-cases, scenarios and derived requirements with respect to the SecureCloud platform.

The structuring of the work packages 2, 3 and 4follows the layered architecture of the SecureCloud platform.

WP2 Infrastructure services to enable secure, QoS-aware applications works at the lowest layer and designs and implements secure containers. The containers will make use of various kinds of hardware support offered by the underlying platform for supporting security, trust, and virtualisation. As the developed components directly interact with the hardware they will also contain parts which monitor the hardware usage to detect resource bottlenecks and allow accounting and billing.

WP3 Dependable Micro-services for the Cloud will utilise the secure containers developed within WP2 to develop a framework for secure micro-services. These micro-service will be executed within the secure containers. The overall output of WP3: on the one hand it will be the framework and the related interfaces allowing to develop arbitrary micro-services on the other hand WP3 will implement a few common Micros-service, e.g. related to storage and networking. These Micro-services can be utilised by the big data processing framework developed within WP4.

The output ofWP4 Secure distributed big data application with micro-services constitutes the next level of abstraction. WP4 will provide components which are specifically addressing big data processing. These components are building using the micro-service framework as well as the common micro-services developed by WP3. The big data processing components will be leveraged by the application level demonstrators developed within WP5. Examples of components developed within WP4 are secure structured data stores, map/reduce based computations, schedulers, as well as components for efficient transmission of large amount of data.

The overall component development methodology will follow the AGILE software development method whereas WP1 Requirements, specification, and design of the SecureCloud platform will be the central steering point. Thus the task of WP1 is to collect an initial set of requirements based on the use-case of WP5, the input from end-users and cloud providers as well as the component WPs. Based on these requirements a first overall design (architecture) of the SecureCloud platform will be created. This leads especially to a first set of well-defined interfaces between the components at the different layers. Immediately afterwards the development of the components within WP2, WP3, WP4 as well as the demonstrators start in parallel. The results of WP2, WP3, and WP4 will be delivered continuously to WP1 for continuous integration and testing. These will allow identifying problems quickly and reacting accordingly by adapting the requirements, the overall design and the interface specifications. Meaningful snapshot of the SecureCloud platform will be provide to WP5 for the development of the demonstrators. The final result of WP1 will be a comprehensive description of the consolidate SecureCloud platform design including consistent and well-defined interfaces between its components.

### Timing of the different WPs and their components (GANTT Chart)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP1** | **Requirements, specification, design of the SecureCloud platform** |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T1.1 | Definition of use cases and requirements |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T1.2 | Design and specification |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T1.3 | Infrastructure for continuous integration |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T1.4 | Continuous assessment |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP2** | **Infrastructure services to enable secure, QoS-aware applications** |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  | ■ |  |  |  |  |  |  |
| T2.1 | Evaluation of technology trade-offs |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T2.2 | Management and lifecycle of secure containers |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T2.3 | Trust management |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T2.4 | QoS monitoring and enforcement |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP3** | **Dependable Micro-services for the Cloud** |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T3.1 | Framework for restartable secure micro-services |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T3.2 | Set of reusable secure micro-services |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T3.3 | Dependability management |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T3.4 | Templated programming model for secure micro-services |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP4** | **Secure distributed big data application with micro-services** |  |  |  |  |  |  |  |  | ■ |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T4.1 | Secure distributed communication mechanisms |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T4.2 | Secure distributed data management and storage |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T4.3 | Distributed scheduling mechanisms |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T4.4 | Secure map/reduce computation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP5** | **Demonstration and Evaluation** |  |  | ■ |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T5.1 | Data preparation for validation of developed algorithms |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T5.2 | Development of monitoring and control applications for smart grids |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T5.3 | Test and validation of secure applications for privacy-sensitive data |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T5.4 | Tests and validation of applications with strict QoS requirements |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP6** | **Dissemination, Exploitation and Communication** |  |  | ■ |  |  | ■ |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T6.1 | Dissemination of project results, and clustering activities |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T6.2 | Market Analysis and Business Plan |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T6.3 | Project Public Web site |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T6.4 | Open Standardization Activities |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Project months:** | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| **WP7** | **Project Management** |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ■ |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | ■ |
| T7.1 | Project coordination |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T7.2 | Administrative, financial and legal management |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T7.3 | Internal website and communication Tools |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Milestones** | |  |  |  |  |  |  |  |  | ▲ |  |  |  | ▲ |  |  |  |  | ▲ |  |  |  |  |  |  | ▲ |  |  |  |  |  |  |  | ▲ |  |  |  |

■ Deliverable ▲ Milestone

Table 3.1‑1: Gantt Chart

### Detailed description of work packages

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **WP no.** | 1 | | **Start Date or Starting Event** | | | | | | | | | | | M1 | |
| **WP title** | Requirements, specification, and design of the SecureCloud platform | | | | | | | | | | | | | | |
| **Participant number** | **1** | 2 | 3 | 4 | 5 | 6 | 7 | **8** | 9 | 10 | 11 | 12 | 13 | 14 | **Total** |
| **Name of participant** | **TUD** | IMP | UniNE | CC | SYNC | IEC | CS | **LACTEC** | UFCG | UTFPR | UNIFEI | COPEL | CAS | INM |
| **PMs** | **13** | 1 | 1 | 2 | 12 | 2 | 5 | **9** | 3 | 3 | 3 | 3 | 3 | 3 | **63** |

|  |
| --- |
| **Objectives**  The objectives of this WP are:   * to define the use cases and to collect the requirements on the overall SecureCloud platform, especially considering the end-user requirements, * to design the overall architecture of the system and to define the components to be developed within WP2, WP3, and WP4 * to assure the integration of all components into a common cloud platform and to setup an infrastructure for continuous integration * to design and implement a test plan and a test bed supporting the continuous evaluation of the components developed, and the SecureCloud platform as a whole. |

|  |
| --- |
| **Description of work**  This work package will collect and coordinate the results to assure development of a comprehensive and secure cloud platform. At first, it will define the use cases, and collect end-user requirements. Here it will interact with WP5 (Demonstrators). It will derive the technical, functional, and non-functional requirements from the use case descriptions, scenario specifications and user requirements. Based on that it will devise and specify the system architecture. It then takes the lead in defining all the relevant components and their interfaces to be developed within WP2, WP3, and WP4. After the development of these components has started this WP monitors and assists the continuous integration of all SecureCloud components to ensure the seamless interoperability of the various developed algorithms, modules, and protocols. Finally, this WP develops a test plan and implements a test bed to allow for continuous evaluation of the SecureCloud platform regarding technical parameters and non-functional requirements.  **Task 1.1: Definition of use cases and requirements** (M1-M9; TUD, CC, SYNC, IEC, CS, LACTEC, UFCG, UTFPR, UNIFEI, COPEL, CAS, INM)  This task involves the explicit design and description of uses cases for the SecureCloud platform considering and deriving end-user requirements. Based on these use-cases and end-user requirements the technical, functional, and non-functional requirements will be deduced.  **Task 1.2: Design and specification** (M2-M36; TUD, IMP, UniNE, CC, SYNC, UFCG)  This task will provide a detailed and open SecureCloud specification. It will furnish a fine-grained system architecture and its interoperability. It will specifically consider the existing OpenStack and Docker architecture and components and extend them as necessary. Grouping the necessary functionality, it will devise a component model as a high-level architecture defining different components. Moreover, Task 1.2 will define all the necessary interfaces between the components resulting in a fine-grained architecture description. This task iteratively intertwines with WP2, WP3, and WP4 as well as Task 1.3 and Task 1.4 resulting in a continuously updated architecture description if necessary.  **Task 1.3: Infrastructure for continuous integration** (M3-M33; TUD, SYNC, CS)  Task 1.3 will watch over the integration of all algorithms, protocols, and components of the SecureCloud platform. It will therefore provide an infrastructure for continuous integration using automated continuous integration toolsets such as Jenkins. We will therefore extend Jenkins for continues integration tests of distributed infrastructures such as the cloud stack developed within the SecureCloud project. The extensions will be carried out using the provided plugin architecture of Jenkins. The plugins and developed integrations test will continuously monitor the quality of software development process and provide an early feedback to WP2, WP3 and WP4 as well as Task 1.2 resulting in an updated architecture description if needed.  **Task 1.4: Continuous assessment** (M4-M33; TUD, SYNC, CS, UFCG)  Task 1.4 develops a test plan allowing continuous evaluation of the SecureCloud platform regarding technical parameters and non-functional requirements. Therefore Task 1.4 will implement a test bed allowing automated testing under realistic conditions. This evaluation will give an early and continuous feedback to the technical developments executed in WP2, WP3, and WP4. |

|  |
| --- |
| **Deliverables**  **D1.1: Requirements & Architecture specification – initial version (**M9; TUD)  This report will contain an initial description of the uses-cases and scenarios. It will list end-user requirements as well as technical, functional and non-functional ones. A coarse description of the architecture and the components of the SecureCloud platform will be included.  **D1.2: Requirements & Architecture specification – intermediate version (**M21; TUD)  Besides a refinement of the uses-cases and the requirements, this report will contain a detailed description of the fine-grained architecture of the SecureCloud platform including all the interfaces between the components.  **D1.3: Requirements & Architecture specification – final version (**M36; TUD)  This report contains the final uses-cases, requirements and fine-grained architecture of the SecureCloud platform incorporating the lessons learned from the execution of WP5 demonstrators. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **WP no.** | 2 | | | **Start Date or Starting Event** | | | | | | | | | | | | M1 | |
| **WP title** | Infrastructure services to enable secure, QoS-aware applications | | | | | | | | | | | | | | | | |
| **Participant number** | 1 | 2 | 3 | | 4 | 5 | 6 | 7 | 8 | **9** | 10 | 11 | 12 | 13 | 14 | | **Total** |
| **Name of participant** | TUD | IMP | UniNE | | CC | SYNC | IEC | CS | LACTEC | **UFCG** | UTFPR | UNIFEI | COPEL | CAS | INM | |
| **PMs** | 13 | 9 | 7 | |  | 2 |  | 8 |  | **62** |  |  |  |  |  | | **101** |

|  |
| --- |
| **Objectives**  This work package will implement infrastructure services that enable the development of application and higher abstraction platform services that are both secure and QoS aware. More specifically, there following objectives will be addressed:   * Scheduling and provisioning services that are aware of secure enclaves; * Monitoring services that enable adequate account and billing for the usage of secure containers; * Enhancement of existing monitoring and orchestration functionalities to enable fast reaction to potential quality-of-service deteriorations.   The services will be implemented in OpenStack, the major open-source middleware for managing cloud infrastructures, enabling a shorter time-to-market for project results. |

|  |
| --- |
| **Description of work**  This work package is led by UFCG, but with a tight cooperation with other partners as described below. The tasks in this WP will design and implement the basic cloud infrastructure services that provide provisioning, scheduling, networking, and monitoring of the basic resources the enable the secure containers.  **Task 2.1: Evaluation of technology trade-offs** (M1-M12; UFCG, TUD, IMP, UniNE, CS)  In this task, the partners will evaluate technologies for implementing secure resources in servers owned by a cloud provider. This set of technologies includes both already in-the-market alternatives (such as the ones targeting secure boot, based on the TPM specifications and supported by major hardware producers) and upcoming features (for example, Intel SGX). As a result of this task, a set of basic services and the respective APIs will be defined to access secure resources. These APIs are agnostic to the cloud middleware being used. The definitions of the services to be provided and the APIs will be the base for the following tasks.  **Task 2.2: Management and lifecycle of secure containers** (M1-M12; UFCG, TUD, IMP, CS)  This task will design and implement the services that enable the management of secure containers in a cloud middleware. It will also include the needed accessory services for (1) scheduling of secure containers, (2) accounting of resource usage for quota management and/or billing, (3) networking of secure containers with software defined networking (SDN).  **Task 2.3: Trust management** (M12-M30; UFCG, TUD, IMP, SYNC, CS)  In this task, the services for configuration of access policies for the APIs that manage secure containers will be developed. This implementation will follow the highly-granular Role-Based Access Control (RBAC) strategy currently used by OpenStack. In addition, the APIs for configuring access and sharing of secure resources will be implemented.  **Task 2.4: QoS monitoring and enforcement** (M12-M30; UFCG, TUD, UniNE)  Enabling quick reaction of applications and higher-level platform services in order to preserve QoS of applications running in a secure cloud environment depends on detailed collection of metrics of the underlying physical resources. At the same time, simply increasing the level of detail of existing metrics (e.g., sub-second sampling of CPU, network and disk usage) will make the timely analysis and reaction to relevant events impossible. Therefore, the monitoring service will need to consider novel approaches for eliminating low-value data. These approaches will have to be user-configurable, but will need to provide scalable and timely processing of a large diversity of metrics and, at the same time, provide responsive orchestration capabilities to enable adequate enforcement of QoS goals. |

|  |
| --- |
| **Deliverables**  **D2.1: Analysis of existing technologies** (M12; TUD)  Analysis of existing hardware technologies for supporting secure processing and a project of services APIs that define how these technologies can be exploited in the context of secure cloud computing.  **D2.2: Prototype services for basic management of secure resources** (M24; UFCG)  This prototype will enable application and higher-level services prototypes to use the secure resources in the context of cloud computing. The first services will enable creation, deletion, accounting and scheduling of secure resources.  **D2.3: Services for trust management for secure resources** (M30; UFCG)  This prototype will enable application and higher-level services prototypes to use the secure resources in the context of cloud computing. The first services will enable creation, deletion, accounting and scheduling of secure resources.  **D2.4: Monitoring and orchestration services for large, high-responsive applications** (M30; UFCG)  As described above, a new approach for monitoring and orchestration services will be implemented to enable fast reaction and QoS enforcement for applications that require both QoS and secure analytics with low response times. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **WP no.** | 3 | | **Start Date or Starting Event** | | | | | | | | | | | | M1 | |
| **WP title** | Dependable Micro-services for the Cloud | | | | | | | | | | | | | | | |
| **Participant number** | 1 | **2** | 3 | 4 | 5 | 6 | 7 | 8 | **9** | 10 | 11 | 12 | 13 | 14 | | **Total** |
| **Name of participant** | TUD | **IMP** | UniNE | CC | SYNC | IEC | CS | LACTEC | **UFCG** | UTFPR | UNIFEI | COPEL | CAS | INM | |
| **PMs** | 20 | **28** | 10 |  |  |  |  |  |  |  |  |  |  |  | | **58** |

|  |
| --- |
| **Objectives**  This work package will provide a framework for developing secure micro-services and implement a set of reusable secure micro-services that will execute within secure containers. The micro-services will be dependable, permitting their automatic restart after failure due to a stateless design. More specifically, the work package will result in the following outcomes:   * Definition and implementation of a service framework that uses secure containers to execute secure micro-services and provides a trusted API to them; * Development of a set of secure micro-services, which will be composable into distributed secure big data applications, as developed in WP4; * Design and implementation of dependability mechanisms for secure micro-services that detect failures of micro-services and restart them transparently; and * Exploration a template model for secure micro-services that facilitates the development of new types of micro-services. |

|  |
| --- |
| **Description of work**  This work package is led by IMP, with contributions by TUD on dependability aspects, and by UniNE on the framework design and secure micro-service implementation.  **Task 3.1: Framework for restartable secure micro-services (incl. implementation)** (M1-M36; IMP, TUD)  This task will develop a framework that supports the implementation and life-cycle of secure micro-services. The framework will expose a trusted API that micro-services can use to interact with the outside world and perform other privileged operations, which would otherwise be not available within a secure container. The design of the API will be inspired by small hyper-call APIs, as exposed by modern hypervisors. In addition, the framework will support functionality to deploy new micro-services, monitor their execution, restart them and destroy them after completion.  **Task 3.2: Set of reusable secure micro-services (incl. implementation)** (M1-M36; IMP, TUD, UniNE)  This task will design and implement a set of reusable secure services that will be useful across a range of secure applications, including the distributed big data applications from WP4. The generic secure micro-services will include (i) a *secure message broker* that will permit different micro-service to communicate according to a topic-based publish/subscribe model; (ii) a *secure identity micro-service* (similar to KeyStone in OpenStack deployments) that enables principals to prove their identify to other micro-services; (iii) a *secure key/value store* that enables the storage of information while preserving confidentiality and integrity; (iv) a *secure coordination micro-service* that provides a consistent namespace abstraction similar to ZooKeeper that is used for synchronisation and coordination; and (v) a *secure task executor micro-service* that permits the execution of secure compute tasks such as mapper and reducers.  **Task 3.3: Dependability management** (M1-M36; TUD, IMP, UniNE)  This task will explore how secure micro-services can be made dependable in practice. The general approach will be to make all secure micro-services stateless, with any required state being maintained outside of the micro-service, e.g. using the secure key/value store. A failure detector as part of the micro-service framework will monitor the liveness of the service. After a failure was detected, the framework will restart the micro-service transparently. We will validate the performance impact of failure recovery on the processing performance of the distributed big data applications from WP4.  **Task 3.4: Templated programming model for secure micro-services** (M1-M36; IMP, TUD, UniNE)  This task will provide an intuitive programming model for new types of secure micro-services. The task will enable developers of secure applications to customise existing micro-services and facilitate the implementation of new micro-services. Developers will follow a templated approach, in which there are pre-defined micro-service classes that target particular functions such as secure data computation, secure communication, secure data storage etc. The main novelty of this approach will be that it will focus on preserving data confidentiality and integrity when defining the functionality of micro-services. This will enable the creation of secure services that are *safe-by-design*, without introducing vulnerabilities e.g. by an incorrect usage of the framework API. |

|  |
| --- |
| **Deliverables**  **D3.1: Specification and implementation of the micro-service framework and API** (M12; IMP)  This deliverable will describe the micro-service framework and document its associated API that will be used to implement micro-services. It also will provide a preliminary implementation of the micro-services and API.  **D3.2: Specification and implementation of reusable secure micro-services** (M24; IMP)  This deliverable will describe the five generic secure micro-services that are developed by Task T3.2. It will provide as well an implementation of the micro-services with its feature-frozen API.  **D3.3: Description of dependability mechanism used by the micro-service framework** (M36; TUD)  This deliverable will describe the dependability approach used to make micro-services robust to failures.  **D3.4: Description of programming model for new micro-services** (M36; IMP)  This deliverable will describe the programming model for new micro-services that makes them safe-by-design. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **WP no.** | 4 | | **Start Date or Starting Event** | | | | | | | | | | | | M1 | |
| **WP title** | Secure distributed big data application with micro-services | | | | | | | | | | | | | | | |
| **Participant number** | 1 | 2 | **3** | 4 | 5 | 6 | 7 | 8 | 9 | **10** | 11 | 12 | 13 | 14 | | Total |
| **Name of participant** | TUD | IMP | **UniNE** | CC | SYNC | IEC | CS | LACTEC | UFCG | **UTFPR** | UNIFEI | COPEL | CAS | INM | |
| **PMs** | 2 | 16 | **33** | 22 |  |  |  |  |  | **6** |  |  |  |  | | **79** |

|  |
| --- |
| **Objectives**  This work package aims at designing and implementing building blocks for developing big data applications on top of micro-services (WP3), themselves deployed within containers (WP2) in the cloud. The main objectives are to make the development of cloud-based big data application easier, safer, and faster. More specifically, the work package will result in the following outcomes:   * T4.1: Secure and efficient (i.e., low latency and high throughput) communication mechanisms for transmitting big data between micro-services, and between clients and big data applications. * T4.2: Distributed scheduling mechanisms designed for executing computation tasks (running in micro-services) close to the data they depend on, and for placing data close to associated compute tasks or to related data for better efficiency. * T4.3: A secure distributed key/value data store for big data application to store their data, and used by the map/reduce framework of T4.4 to store (intermediary) computation results. * T4.4: A generic framework for map/reduce computations with big data across micro-services, as well as a collection of pre-defined components for big data processing.   This workpackage is led by UniNE, with significant technical contributions from TUD, IMP, and CC. |

|  |
| --- |
| **Description of work**  This work package is led by IMP, with contributions by TUD on dependability aspects, and by UniNE on the framework design and secure micro-service implementation.  **Task 4.1: Secure** **distributed communication mechanisms** (M1-M36; UniNE, IMP, CC)  This task focuses on the development of secure and efficient communication mechanisms for transmitting big data between micro-services, and between clients and big data applications. Efficiency will be measured in terms of latency and throughput: for tasks that require short response times, latency must be optimized at the price of sending small data packets; for jobs that must access large amounts of data that might not be available locally, focus will be on throughput. Communication will take place using a message bus. The communication mechanisms will be designed from the ground up for security by using encryption and authentication at the level of micro-services. Simple APIs will be provided for micro-services and clients to use the communication primitives in a language-agnostic manner.  **Task 4.2:** **Secure distributed data management and storage** (M1-M36; CC, IMP, UniNE, UTFPR)  This task comprises the development of distributed data management and storage mechanisms that exploit the properties of network coding. The basic idea is that, when data is encoded and stored in different locations (typically clouds), data privacy is ensured as long as an attacker does not compromise (break into) enough of these locations. Furthermore, additional levels of security can be introduced to protect the data even if many clouds are compromised. A first level involves encrypting the encoding coefficients of random linear network coding (information about how the packets were combined in order to recover) using standard techniques, e.g., AES, RSA. This approach relies on the fact that random linear network coding is a cipher as long as the encoding coefficients are not revealed. A caveat is that the encryption of each coded packet can be attacked as each cloud is compromised, although no data is revealed until all encryptions and sufficiently clouds are compromised. A second level, involves encrypting the data prior to encoding for introducing an additional level of privacy (as used in T4.2 to protect communication). The attacker will only be able to attack the encryption of the data after gaining access to each cloud provider. A third level includes a combination of the two previous approaches.  The outcome of this task will be a data store with a key/value APIs for securely storing data using the security mechanisms described above. It will be able to store data of arbitrary size (both small and massive) to match the requirements of big data processing, and will leverage the secure distributed communication mechanisms of T4.1 for transmitting data between clouds.  **Task 4.3: Distributed scheduling mechanisms** (M12-M36; UniNE, TUD, IMP, CC)  Big data processing requires accessing massive amounts of data. It is therefore of uttermost importance to co-locate computations with the data they need to access or process. This task will focus on the scheduling of tasks so that they can be placed nearby the data they need to access, when possible and applicable. It will also provide mechanisms for migrating or replicating (i.e., creating another copy) of data to move it closer to the tasks that process it. In the latter case, the task will leverage the secure distributed communication mechanisms of T4.1 for transmitting data. As the content of the data is irrelevant for scheduling, there is no need to decrypt data. It is important, however, to guarantee that moving data from one cloud to another does not compromise security by reducing the number of clouds that an attacker needs to break into; therefore this task will rely on guidance from T4.2 to decide upon placement data (and hence scheduling of tasks) across clouds.  **Task 4.4: Secure map/reduce computation** (M1-M36; UniNE, IMP, TUD, CC)  Map/reduce (and its “dynamic” evolutions supporting data streams) is one of the most widely used programming model for big data processing. It essentially relies on two phases: data is first split and processed in parallel, and the results of the first phase are then combined to complete the computation. A map/reduce framework provides a set of basic services for orchestrating the computation across distributed servers, including lifecycle of mappers and reducers, storage of intermediary results, transmission of data across servers, and synchronization of the various participants. This task will provide a simple implementation of a map/reduce framework tailored for the micro-service architecture of SecureCloud, leveraging the communication mechanisms of T4.1, the secure data store of T4.2, and the scheduling mechanisms of T4.3. |

|  |
| --- |
| **Deliverables**  **D4.1:** **Specification and design of** **the** **micro-services for distributed big data applications** (M9; UniNE)  This deliverable will conclude the design phase in WP4. It will specify the interfaces and semantics of the main components of the work package, namely the secure communication, distributed storage, and map/reduce libraries.  **D4.2: Preliminary implementation of the communication and storage mechanisms** (M12; CC)  This deliverable will provide a preliminary implementation of the communication and storage mechanisms (with complete API support but no security/dependability features).  **D4.3: First** **implementation of the micro-services for distributed big data applications** (M24; UniNE)  This deliverable will contain the final implementation of the secure communication mechanisms, an advanced implementation of the distributed data store (with security but without privacy-aware scheduling support), a first prototype of the secure map/reduce framework, and basic scheduling mechanisms (not privacy-aware).  **D4.4: Integrated implementation of the micro-services for distributed big data applications** (M36; UniNE)  In this deliverable, the final implementations of the secure communication, distributed storage, map/reduce, and scheduling components of WP4 will be provided. These final versions will have been validated using continuous integration and validation mechanisms of WP1 and using use cases of WP5. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **WP no.** | 5 | | | **Start Date or Starting Event** | | | | | | | | | | | M1 | | |
| **WP title** | Demonstration and Evaluation | | | | | | | | | | | | | | | | |
| **Participant number** | 1 | 2 | 3 | | 4 | 5 | **6** | 7 | **8** | 9 | 10 | 11 | 12 | 13 | | 14 | **Total** |
| **Name of participant** | TUD | IMP | UniNE | | CC | SYNC | **IEC** | CS | **LACTEC** | UFCG | UTFPR | UNIFEI | COPEL | CAS | | INM |
| **PMs** | 4 | 1 | 1 | | 2 | 17 | **5** | 4 | **32** | 12 | 31 | 22 | 2,5 | 27,5 | | 24 | **185** |

|  |
| --- |
| **Objectives**  The objective of the work package 5 is to build a proof of concept of the application of the SecureCloud platform for secure and privacy-respecting big-data processing using data from real smart metering pilots. The main idea is to validate the use of the SecureCloud platform for the execution of smart metering algorithms, including billing, fraud detection, energy balance, energy delivering and fault detection, load shedding, among others. Due to fraud attempts in energy meters and metering communication systems, applications of smart metering in Brazil have become preferred targets to attacks. Therefore, cloud computing must be ensured as a secure technique for Smart Grid applications. The credibility of cloud computing for such applications will be tested and validated by implementations using the SecureCloud platform for the execution of applications in secure containers. The validation will use data taken from real smart metering systems, acquired from distribution utilities and smart grid pilots. These data will be used for smart metering algorithms creation, tests and validation as well as creation and validation of applications of secure containers for cloud computing. Moreover the validation will utilise a close-to-real-world SmartGrid testbed provided by IEC. In this way, WP5 will validate the innovation and effectiveness of the platform methodolo­gy developed during the project. The validation process will be set up in order to demonstrate the results achieved and the breakthroughs of the solution provided in SecureCloud. For this purpose the following efforts will be implemented during the WP5:   * Define an effective set of Key Performance Indicators (KPI), for assessing the impacts of the SecureCloud platform concerning: the mitigation of the cyber-attack risks, the capability to prevent cyber-attacks, the capability to detect cyber-attacks. * Plan and execute extensive test cases in reduced real scenarios with the involvement of each utility and the IEC SmartGrid testbed in order to carry on the validation and test of the SecureCloud findings. * Define and create specific smart metering algorithms to be processed at the cloud; * Ensure properties of integrity, authenticity and confidentiality through the validation of embedded secure modules in smart meters; * Application of smart metering data processing through secure containers; * Validate the SecureCloud platform  by testing the performance of the application of smart metering algorithms for a real workloads, using the SecureCloud platform; * Validate the security and privacy of the metering data and algorithms, ensuring that both the data and the metering software can run in the cloud in a secure way; * Provide evaluation of the results achieved.   A final report with the validation results and the developed applications will be published. The outcomes of these activities will give useful inputs for an effective exploitation of the solutions developed in the SecureCloud project. |

|  |
| --- |
| **Description of work**  This work package will develop the tasks required for assembling and validating the use cases. The first use case requires private and secure processing of sensitive data. The second requires timely processing of data from the grid, such that reaction to relevant events is executed in a timely fashion. LACTEC, CAS, COPEL and UNIFEI will work on collecting data that will support a testbed for the use cases. These partners, in conjunction to UFCG, UTFPR, INMETRO and IEC will then adapt well-stablish monitoring (and control) algorithms to work efficiently in the proposed cloud infrastructure and platform services. Then, in Task 5.3, a validation plan will be build. After that, the data, the algorithms and the infrastructure will be combine in the two remaining tasks to demonstrate and validate the use cases.  **Task 5.1: Data preparation for validation of developed algorithms** (M1-M3; LACTEC, SYNC, UNIFEI, COPEL, CAS)  This task involves the acquisition and pre-processing of smart grid data in order to prepare the database structures for the development of smart metering applications in the cloud. For example, smart meter data need to be anonymized and data from other sensors, but from different companies will be made uniform, before inserted in the database. These data will be obtained from real smart grid deployments and smart metering pilot projects.  **Task 5.2: Development of monitoring and control applications for smart grids** (M3-M15; LACTEC, UFCG, UTFPR, UNIFEI, CAS)  This task involves the adaptation of algorithms for billing, fraud detection, energy balance, energy delivering, fault detection, among others. These algorithms will be the core of the cloud-native applications that will run on the SecureCloud platform. Cloud-native application efficiently use the cloud services that are offered by the underlying platform. We consider both applications that monitor the smart grid without disclosing sensible information and applications that must react to relevant events with predictable timeliness.  **Task 5.3: Test and validation of secure applications for privacy-sensitive data**(M1-M24; UTFPR, TUD, CC, SYNC, IEC, CS, LACTEC, UNIFEI, CAS, INM)  This task will assembly and demonstrate use case 1: secure and private processing of sensitive data from smart meters. This task includes the adaptation of smart meters developed previously to include secure communication between the meter and the application in the secure cloud. Then, it will validate the security and privacy of the application from end-to-end, from the acquisition of the data, reaching the cloud in a secure way, until the output of the non-sensitive, aggregated data to the interested entity (e.g., the power distribution company).  **Task 5.4: Tests and validation of applications with strict QoS requirements** (M11-M36; UFCG, TUD, IMP, UniNE, CC, SYNC, IEC, CS, LACTEC, UTFPR, COPEL, CAS, INM)  This task will assembly and demonstrate use case 2: secure applications that need to be made robust regarding QoS. In this task, the control application considered in Task 5.2 will be validated, using the realistic workloads the data obtained in Task 5.1. Therefore, this task will assembly and validate the demonstrator for smart grid control applications running in the SecureCloud platform over multiple clouds, for robustness. This task will also consider scalability issues, and, therefore, provide the final template for building secure, robust big-data application in the cloud. |

|  |
| --- |
| **Deliverables**  **D5.1: Database for the testbed that will run smart grid application to the cloud.** (M3; LACTEC)  Database for helping with testing and developed of data-processing applications.  **D5.2: Cloud-native applications for billing, fraud detection, energy balance, energy delivering and fault detection** (M14; LACTEC)  Set of applications that process data from smart grids in the cloud.  **D5.3:** **Demonstrator for the end-to-end secure and privacy-friendly application for smart meter data** (M24; UTFPR)  A demonstrator illustrating a data-processing application that considers data that should be known by neither the application nor the cloud providers.  **D5.4:** **Demonstrator for strict-QoS application with realistic workloads running in a secure cloud** (M36; UFCG)  A demonstrator illustrating a data-processing application that requires robust responsiveness (i.e., applications that actuate on the smart grid). |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **WP no.** | 6 | | | **Start Date or Starting Event** | | | | | | | | | | | M1 | |
| **WP title** | Dissemination, Exploitation, and Communication | | | | | | | | | | | | | | | |
| **Participant number** | 1 | 2 | 3 | | 4 | **5** | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | **Total** |
| **Name of participant** | TUD | IMP | UniNE | | CC | **SYNC** | IEC | CS | LACTEC | UFCG | UTFPR | UNIFEI | COPEL | CAS | INM |
| **PMs** | 2 | 1 | 1 | | 2 | **3** | 1 | 4 | 4 | 2 |  |  |  |  |  | **20** |

|  |
| --- |
| **Objectives**  This work package is designed to increase the impact of SecureCloud on the various communities of interest, specifically: scientists/researchers, industrial entities including SMEs, and other relevant cloud stakeholders (including governments and administrations). The objectives of WP6 can be summarized as follows:   * Manage and promote the successful exploitation of SecureCloud activities; * Ensure great publicity and dissemination of results; * Create and regularly update an Exploitation and Use Plan.   In a nutshell, WP6 overarching goal will be to ensure commercialisation and future sustainability of project outputs. To this end WP6 will benefit from the participants’ existing networks to form a triple-helix collaboration commitment among leading companies, research centres, and universities and to cluster with relevant funded projects in Europe in alignment with the aims of Horizon2020. |

|  |
| --- |
| **Description of work**  This WP will be led by Sync Lab with substantial contributions being provided by all other partners.  **Task 6.1: Dissemination of project results, and clustering activities** (M3-M36; SYNC, TUD, IMP, UniNE, CC, LACTEC, UFCG)  The goal of this task, led by Sync Lab and involving all partners, is to advertise and publicise as much as possible project activities and outcomes. The consortium will extend the means of disseminating project results beyond the traditional ones (i.e. web-based dissemination and participation of academic partners in conferences/workshops as well as publication of project results in top ranked scientific journals). Effective social media campaigns will be performed to promote via social networks (and in particular: Facebook, Twitter, Google+, and LinkedIn) and Internet media channels (specifically: YouTube) the achievements of the project in several domains. Forums and blogs with high traffic, relevant to the pilot domain, will also be a main target of the dissemination actions. Printed materials (brochures, posters, and giveaways) will also be produced and distributed at selected events.  A data management plan will be provided early on (by month 6) that details the specifics on how the results (quite valuable data) will be made available for the community.  The consortium - and in particular the pilot leader - aim at organizing exhibitions and workshops at the regional level, where they will invite stakeholders and major players in the field of the pilot, within and outside the European Union.  Two major events are foreseen for the whole duration of the project in the form of workshops, the first organized shortly after the start of the project and the second one close to the end of the project. The addressed audience will include - but will not be limited to - scientific, research, and market communities focusing on specific market segments included in the SecureCloud pilot domain, as well as in the cloud market in general. The basic aim of the first workshop will be to gather additional requirements for the implementation of the SecureCloud framework, whereas the second workshop will serve as a presentation of the project outcomes to a wider audience.  **Task 6.2: Market Analysis and Business Plan** (M24-M36; SYNC, TUD, CC, CS)  The key objective of this task is to perform a thorough market analysis for the individual security features, as well as for the entire solution proposed, in the potential market segments targeted by the SecureCloud project. A preliminary market analysis will focus on the pilot business domain, which will then be extended to the cloud computing market in general.  An exploitation plan will be developed and constantly updated throughout the lifetime of the project, in order to prepare, support, and present business initiatives and opportunities created by the project. Updates of the initial plan will be included as separate parts of the progress reports. This task will also deliver the Final Exploitation and Use Plan, that will describe the participants’ actual achievements and their commercialization plans for the exploitable assets developed within the project. Business Modelling – creation of sustainable and financially profitable scenarios – will form a large part of this process and in order to facilitate it, multiple business workshops and interviews will be held with SMEs and large industrial players in the relevant areas.  **Task 6.3: Project Public Web site** (M1-M36; SYNC, TUD)  The SecureCloud official Web site will play a major role in the dissemination of project results, as well as in interaction with the PO and the EC. Information will be classified into: public, private, and restricted. The Web site will include a Content Management System (CMS), support RSS feeds, and host a blog. Four roles are foreseen for the project: Public, Partner, Project Officer (PO), and Reviewer. The blog will allow partners, users, and developers to communicate and share their ideas. The RSS feeds will allow people to receive timely updates on project activities and results.  **Task 6.4: Open Standardization Activities** (M24-M36; SYNC, TUD, CS)  The goal of this task is to closely monitor the main standards and/or standardization activities that are relevant for cloud computing security, and in particular those identified in ENISA document “Cloud Standards and Security”. The work of the main standardization bodies and technical committees will be followed closely, to ensure that results be used in SecureCloud where possible. Also importantly, some of the partners of the consortium have been active contributors for several years to specific standardization bodies, where they are willing to promote the scientific results of SecureCloud. In particular, Some of the researchers of Sync Lab team are actively involved in ETSI and IETF standardization activities and are willing to contribute to ETSI Cloud Technical Committee and IETF initiatives on cloud computing. |

|  |
| --- |
| **Deliverables**  **D6.1: Project web site** (M3; SYNC)  The project website is set up and put on-line. Every six months a snapshot of the Web site will be made and released as a DVD (possibly in bundle with additional dissemination materials). (Contributing task: T6.3)  **D6.2: Data Management Plan** (M6; SYNC)  This report includes the procedures to manage the data gathered in the demonstrators. This deliverable will evolve during the lifetime of the project in order to present the status of the project's reflections on data management.  **D6.3: Project dissemination and clustering activities report** (3 versions due M12, M24 and M36; SYNC)  Report (annual) on the dissemination actions taken to promote the main project achievements, as well as interactions/synergies with related research initiatives. Small publication, containing highlights on major project achievements in the reporting period. Language style will be oriented to the public audience at large. (Contributing task: T6.1)  **D6.4: Project exploitation and use plan** (2 versions due M24 and M36; SYNC)  Report (two releases, the first in M24 and the second in M36) on the market analysis and business plans by the involved partners associated with the specific market segments of the SecureCloud pilot domain as well as the SecureCloud potential market in general. Contributing task: T6.2.  **D6.5: Standardization activities** (M36; SYNC)  Report on the activities undertaken for maximizing SecureCloud impact in terms of: i) industrial take-up, by ensuring that the proposed technology be compliant to the emerging standards in the field, and ii) contribution to standards, by approaching standardization bodies and possibly contributing to their work. Contributing task: T6.4  **D6.6: Periodic research newsletter** (3 versions due M12, M24 and M36; SYNC)  Jargon-free on-line publications providing direct and timely updates on project highlights. Contributing tasks: T6.1, T6.2. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **WP no.** | 7 | | **Start Date or Starting Event** | | | | | | | | | | | | M1 | |
| **WP title** | Project Management | | | | | | | | | | | | | | | |
| **Participant number** | **1** | 2 | 3 | 4 | 5 | 6 | 7 | **8** | 9 | 10 | 11 | 12 | 13 | 14 | | **Total** |
| **Name of participant** | **TUD** | IMP | UniNE | CC | SYNC | IEC | CS | **LACTEC** | UFCG | UTFPR | UNIFEI | COPEL | CAS | INM | |
| **PMs** | **14** |  | 1 |  | 1 | 1 |  | **18** |  |  |  |  |  |  | | **35** |

|  |
| --- |
| **Objectives**  The project coordinator of the European consortium—Prof. Christof Fetzer (TUD-SE)—is the interface between the consortium and the European Commission; Rodrigo Riella (LACTEC) is the coordinator of the Brazilian team and the interface towards CTIC (RNP); both ensure a proper project organisation internally as well as with external bodies. They are closely working together with an Administrative Manager (TUD-EPC). Together they form the Project Management Team (PMT).  The key objectives are to:   * Ensuring highest **quality of research activities** and to **streamline the research and development activities** carried out by the different partners, organized and coordinated within the different work packages; * Ensuring the project's implementation within the targets of t**ime, budget and quality and the achievement of objectives**; * Providing a **management structure for a transparent and effective communication and decision-making** between the partners while establishing and maintaining a **high level of team spirit and esprit de corps**; * Providing the **interface between the European Commission** (for the European consortium) respectively **CTIC (RNP)** (for the Brazilian consortium) and other stakeholders for communication ensuring visibility of the project; * Providing the **interface for the Advisory Committee** in order to involve this body in major decisions within the project and ensure efficient communication of relevant issues and information.   All tasks will be accomplished by using state of the art management instruments and methods. This should facilitate an unobstructed and successful project and research evolution. |

|  |
| --- |
| **Description of work**  The following is a list of the tasks required to achieve the objectives of this work package. The management structure as well as the individual roles and responsibilities within this structure are explained in Section 3.2. The section includes a brief overview of the most important procedures that will be constantly refined during the course of the project.  **Task 7.1: Project coordination** (M1-M36; TUD-SE/LACTEC, UniNE, IEC)  Supervision of the research progress considering the scientific objectives targeted by the project. This will include several aspects like   * Ensuring accomplishment of the research and technical objectives, * Quality management and monitoring compliance by the consortium participants with their obligations, verifiable assessment and reviewing of the project against the deliverables and milestones, * Ensuring knowledge transfer among work packages, * Management of risks and conflicts, internal and external reporting, internal dissemination of information; * Preparing and chairing of meetings, preparing minutes of meetings and monitoring implementation of decisions taken at meetings, * Collecting, and (final) reviewing, and submitting technical reports to the European Commission (for the European consortium) respectively CTIC (RNP) (for the Brazilian consortium) according to Description of Action (DoA).   **Task 7.2: Administrative, financial and legal management** (M01-M36; TUD-EPC/LACTEC, SYNC)  Supervision of all related issues regarding legal, financial and administrative issues including   * Legal and contract (change) management of core contract, Technical Annex and Consortium Agreement, * Setting up of a Consortium Agreement and controlling all legal issues and Intellectual Property Rights. For those partners who do not have a dedicated department, TUD (as coordinator) and Sync Lab (as Exploitation and Innovation Manager) will serve as a helpdesk in all questions in respect to protection of knowledge. * Monitoring of work flows and scheduling of work, communication between partners and to the European Commission (for the European consortium) respectively CTIC (RNP) (for the Brazilian consortium); * Collecting, reviewing, and submitting financial reports (including financial statements and related certification) to the European Commission (for the European consortium) and/or CTIC (RNP) (for the Brazilian consortium), budgeting and distribution of money to the partners.   For the European consortium, the European Project Center of TU Dresden (TUD-EPC) will take the main responsibility here and, through its experience, make sure that all reporting requirements by the EC are met in time and with the expected quality.  For the Brazilian consortium, LACTEC will take the main responsibility here and, through their experience, make sure that all reporting requirements by the CTIC (RNP) are met in time and with the expected quality.  **Task 7.3: Internal website and communication Tools** (M01-M36; TUD)  An internal website and communication platform will be established for supporting communication and collaboration between the project partners. This platform will consist of collaboration tools such as a WIKI, shared document folders, an RSS feed and group calendar. The collaboration platform will reside on the SecureCloud website (see WP6) with a login mechanism to control access. |

|  |
| --- |
| **Deliverables**  **D7.1: Project Management Tools** (M03; TUD)  An internal website will be created initially to form a repository of documentary and other information that is relevant to the implementation of the project, and that can also be used to provide an initial intra-project communication system. It can later be extended with an external portal for public results and information; that work will be performed in WP6. Additionally, the usual collaboration tools and procedures (e.g. mailing list) will be installed and made available to the project partners. Further an internal project handbook will be provided that describes the procedures applied to ensure the quality of the project results.  **D7.2: First Periodic Report** (M18; TUD)  This deliverable reports on the achieved results of the project and the overall schedule of tasks. It reports any deviations from the work plan and risks associated with the performed work and planned milestones. It provides further a financial status and its spending.  **D7.3: Final Periodic Report** (M36; TUD)  This deliverable reports on the achieved results of the project and the overall schedule of tasks. It reports any deviations from the work plan and risks associated with the performed work and planned milestones. It provides further a financial status and its spending.  **D7.4: Final Report** (M36; TUD)  This final report summarises the project’s activities over its full duration. This report will cover the main aspects of the work, objectives, results and conclusions. |

### List of Work Packages

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **WP** | **WP title** | **Lead no.** | **Lead participant** | **Person months** | **Start month** | **End month** |
| WP1 | Requirements, specification, and design of the SecureCloud platform | 1 | TUD | 63 | 1 | 36 |
| WP2 | Infrastructure services to enable secure, QoS-aware applications | 9 | UFCG | 101 | 1 | 30 |
| WP3 | Dependable Micro-services for the Cloud | 2 | IMP | 58 | 1 | 36 |
| WP4 | Secure distributed big data application with micro-services | 3 | UNINE | 79 | 1 | 36 |
| WP5 | Demonstration and Evaluation | 8 | LACTEC | 185 | 1 | 36 |
| WP6 | Dissemination, Exploitation and Communication | 5 | SYNC | 20 | 1 | 36 |
| WP7 | Project Management | 1 | TUD | 35 | 1 | 36 |
|  |  |  |  | 541 |  |  |

Table 3.1‑2: List of Work Packages

### List of Deliverables

| **Del. no.** | **Deliverable name** | **WP no.** | **Lead part.** | **Type** | **Dissem.**  **level** | **Delivery month** |
| --- | --- | --- | --- | --- | --- | --- |
| D1.1 | Requirements & Architecture specification – initial version | 1 | TUD | R | PU | 9 |
| D1.2 | Requirements & Architecture specification – intermediate version | 1 | TUD | R | PU | 21 |
| D1.3 | Requirements & Architecture specification – final version | 1 | TUD | R | PU | 36 |
| D2.1 | Analysis of existing technologies | 2 | TUD | R | PU | 12 |
| D2.2 | Prototype services for basic management of secure resources | 2 | UFCG | DEM | CO | 24 |
| D2.3 | Services for trust management for secure resources | 2 | UFCG | OTHER | PU | 30 |
| D2.4 | Monitoring and orchestration services for large, high-responsive applications | 2 | UFCG | DEM | PU | 30 |
| D3.1 | Specification and implementation of the micro-service framework and API | 3 | IMP | DEM | PU | 12 |
| D3.2 | Specification and implementation of reusable secure micro-services | 3 | IMP | DEM | PU | 24 |
| D3.3 | Description of dependability mechanism used by the micro-service framework | 3 | TUD | R | PU | 36 |
| D3.4 | Description of programming model for new micro-services | 3 | IMP | R | PU | 36 |
| D4.1 | Specification and design of the micro-services for distributed big data applications | 4 | UniNE | R | PU | 9 |
| D4.2 | Preliminary implementation of the communication and storage mechanisms | 4 | CC | DEM | PU | 12 |
| D4.3 | First implementation of the micro-services for distributed big data applications | 4 | UniNE | DEM | PU | 24 |
| D4.4 | Integrated implementation of the micro-services for distributed big data applications | 4 | UniNE | R | PU | 36 |
| D5.1 | Database for the testbed that will run smart grid application to the cloud | 5 | LACTEC | OTHER | CO | 3 |
| D5.2 | Cloud-native applications for billing, fraud detection, energy balance, energy delivering and fault detection | 5 | LACTEC | OTHER | PU | 14 |
| D5.3 | Demonstrator for the end-to-end secure and privacy-friendly application for smart meter data | 5 | UTFPR | R | PU | 24 |
| D5.4 | Demonstrator for strict-QoS application with realistic workloads running in a secure cloud | 5 | UFCG | DEM | PU | 36 |
| D6.1 | Project web site | 6 | SYNC | R | PU | 3 |
| D6.2 | Data Management Plan | 6 | SYNC | R | PU | 6 |
| D6.3 | Project dissemination and clustering activities report (3 versions) | 6 | SYNC | R | PU | 12,24,36 |
| D6.4 | Project exploitation and use plan (2 versions) | 6 | SYNC | R | PU | 24,36 |
| D6.5 | Standardization activities | 6 | SYNC | R | PU | 36 |
| D6.6 | Periodic research newsletter (3 versions) | 6 | SYNC | R | PU | 12,24,36 |
| D7.1 | Project Management Tools | 7 | TUD | R | CO | 3 |
| D7.2 | First Periodic Report | 7 | TUD | R | CO | 18 |
| D7.3 | Final Periodic Report | 7 | TUD | R | CO | 36 |
| D7.4 | Final Report | 7 | TUD | R | CO | 36 |

Table 3.1‑3: List of Deliverables

## Management structure and procedures

The primary objective of all management activities in SecureCloud is to guarantee the scientific and technical success of the proposed project and an efficient collaboration between the European and Brazilian project partners. The project’s management structure is based on well-known best practice methodologies and is designed to provide an appropriate level of professional management to mediate efficiently between the different interests and competences of the partners. Its main purpose is ensuring close links between the organization of the work, decision-making and control while at the same time keeping the administrative effort to a minimum despite long distances and time shifts between the European and Brazilian team members. The established management structure will guarantee efficient communication flows within the consortium by taking these issues into account.

The project coordinator (PCO) of SecureCloud will be Technische Universität Dresden (TUD), Chair of Systems Engineering, for the European part. He will be supported by the local Brazilian coordinator (BCO), Institutos Lactec (LACTEC), for the Brazilian part. While TUD will be ultimately responsible for the project management and communication with the European Commission, LACTEC take over this role for the Brazilian consortium in order to synchronise and comply with local requirements stipulated by CTIC (RNP). One work package, WP7 Project Management, is fully dedicated to project management and related activities.

TUD-SE will perform the scientific and technical coordination given their successful participation in previous EU projects (STREAM, VELOX, SRT-15, LEADS, ParaDIME and SERECA) and excellent support infrastructure by TUD-EPC. Professor Fetzer is currently coordinating the Resilience Path of cfAED (center of Advancing Electronics Dresden) and had previously coordinated the SREX (Secure Remote EXecution) project—which was funded by ESF and was successfully completed in 2014.

For the Brazilian part of the consortium, the Lactec Institutes are predestined to be the coordinating institution, due to some factors. The focus of Lactec Institutes are the development of research projects for the energy sector and development of new solutions for the industry, being a self-sustainable entity and having the good development of these research projects as a crucial point for its maintenance. Therefore, Lactec Institutes have the complete knowledge and methodology for managing big research projects, being responsible for dozens of these projects developed in Brazilian energy sector. Specifically in this consortium, Institutes Lactec have, in addition to expertise in the development of applications for Smart Grid, which will be used for validation, a strong interaction with both industrial partners and the universities and research centres participating, being already developed partnership projects with all institutions of the Brazilian consortium. Thus, besides the natural experience in the development and management of research projects, the Lactec Institutes have a great interaction with the other participating institutions, both the academic side as by the industry side, which places it as a natural candidate for the coordination of the Brazilian consortium.

The project coordinator will be supported by the European Project Center (TUD-EPC) with respect to administrative, legal and financial aspects. TUD has extensive experience in project coordination and management. Already in 2005, TUD established the European Project Center to support international project management. Currently, TUD-EPC is coordinating and managing more than 320 projects with a total project volume amounting to over 134 MEUR granted by the European Commission. TUD-EPC supported the development of this proposal. During the implementation of the project, necessary coordination- and management-related activities will be split internally – depending on the required actions – between the Chair of Systems Engineering (TUD-SE) and the European Project Center (TUD-EPC).

A Coordination Agreement will be signed among the European and Brazilian partners to ensure tight coordination of both consortia that aims linking the two projects and ensuring the necessary synergies under a single framework including appropriate arrangements regarding:

* Internal organisation of the beneficiaries in both actions, including decision making procedures;
* Rules on IPR (e.g., protection, dissemination, use and access rights);
* Settlement of internal disputes;
* Liability, indemnification and confidentiality arrangements between both consortia.

Annex I of the proposal contains a draft version of the SecureCloud Coordination Agreement.

### Management Structure

SecureCloud targets an appropriate management structure according to the project size and consortium constellation. An organisational structure with well-defined procedures and decision-making mechanisms will be implemented to ensure the smooth execution of the project. The SecureCloud research and innovation activities are organised in work packages steered by the individual WP leaders and supervised by the Technical Board (TB). Following, the roles of the different bodies and persons involved as well as the principles of our internal communication are outlined (see Figure 3.2-1).

* **Project Management Team (PMT)**, consisting of **Project Coordinator (PCO)**, TUD-SE, local **Brazilian Coordinator (BCO)**, LACTEC, and **Administrative Manager (AM)**, TUD-EPC;
* **Management Board (MB)**, ultimate decision-making body of the consortium, in which each European and Brazilian partner is represented and strategic decisions are taken concerning the entire project and the general course of the work are taken. MB is chaired by the PCO and BCO;
* **Project Boards (PB)**—one at European and one at Brazilian side—for management tasks that are specific due to local requirements and guidelines;
* **Technical Board (TB),** chaired by the PCO and BCO for operative decisions;
* **Advisory Board (AB)**, consisting of representatives from industry, research, public sector, and administration as the gateway between SecureCloud and potential markets as well as other stake­holders, like industry fora and regulatory bodies;
* **Exploitation and Innovation Manager (EIM)** with profound industry-specific knowledge regarding business issues and markets.

Defined tasks and responsibilities will achieve an efficient and effective control of the project on three levels:

* At **strategic level** where the Management Board (MB) will decide the overall strategic orientation of the project, agree plans, monitor milestones (cf. Table 3.2-2) and approve results.
* At **technical and operational level** where the Technical Board (TB) will steer the scientific and technical activities of project and ensure the technical quality of the deliverables of the project.
* At **day-to-day operation** where the Project Management Team (PMT) will conduct the daily affairs.

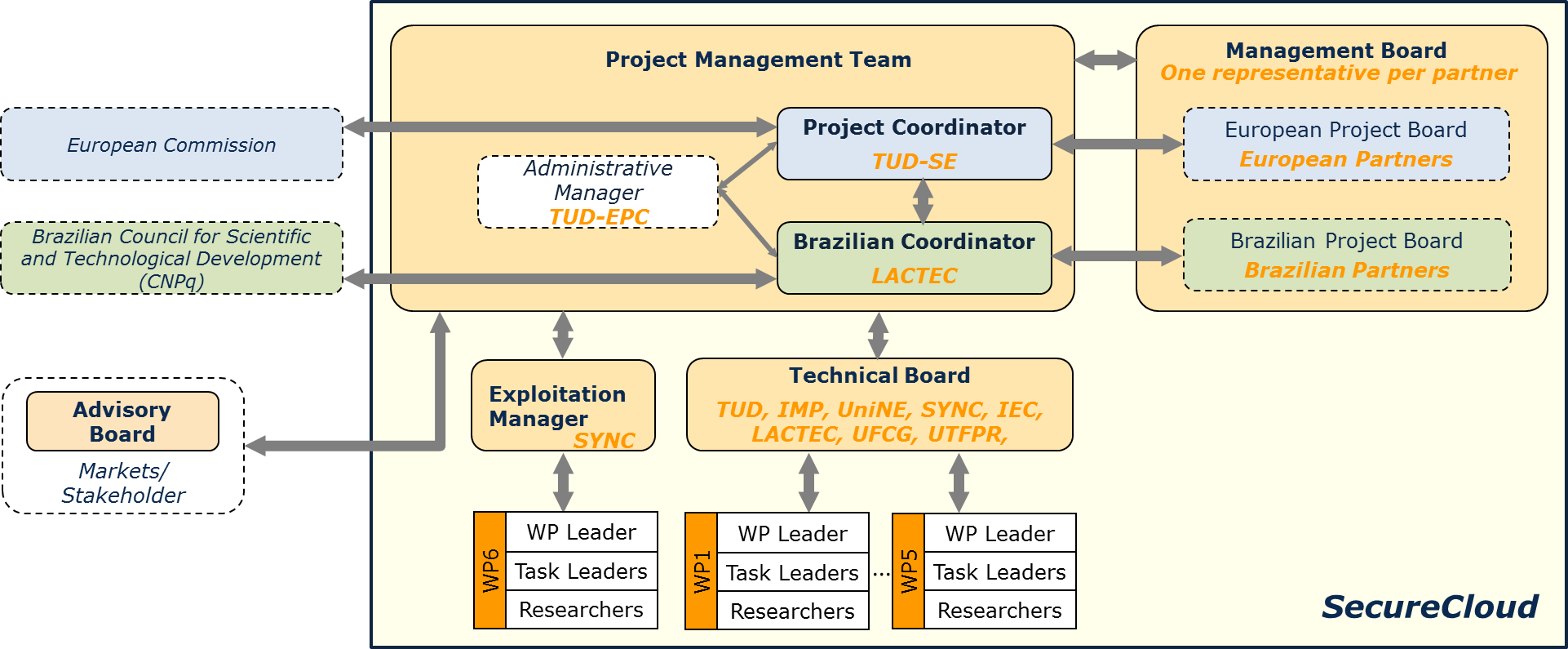


Figure 3.2‑1: SecureCloud Management Structure

#### Project Management Team (PMT)

The **Project Coordinator** (PCO)—Prof. Christof Fetzer (TUD-SE)—is ultimately responsible for project management and is the single point of contact between the European Commission and the European consortium. In this function the PCO shall sign the Grant Agreement with the Commission after all European and Brazilian participants have negotiated and signed the Consortium Agreement. Together with the BCO the PCO defines the high-level technical and scientific strategy and drives the project team to act according to that strategy. In implementing this strategy, the PCO also ensures that the project maintains its relevance to the Horizon 2020 LEIT ICT program and its strategic objectives especially with regards to its objectives towards the European and Brazilian cooperation in the envisaged knowledge domain. In addition, the PCO is responsible for:

* Overall management of the project, including
  + Ensuring that all project objectives are met and that decisions are taken in time;
  + Assuring that decisions taken by the MB are implemented and traced by the TB;
  + Monitoring of the overall progress of the project and verifying the completion of contractual obligations, i.e. milestones (cf. Table 3.2-2) and deliverables (cf. Table 3.1-3).
* Organization and chairing of the meetings and decisions of the MB, TB, AB, and European PB;
* Transmission of documents and information connected with the project between the parties concerned (which does not exclude transmission of the documents and information also directly between parties concerned);
* Ensuring prompt delivery of all deliverable items identified in the contract or requested by the Commission for reviews and audits, including the results of the financial audits prepared by independent auditors, and
* Monitoring the technical quality of the WP output and ensuring the consistency of the output, i.e., technical deliverables and internal reports;
* Synchronisation with the BCO regarding technical progress but also local requirements regarding financing and reporting.

The **local Brazilian** **Project Coordinator** (BCO)—Dr. Rodrigo Jardim Riella (LACTEC)—will act as single point of contact between CTIC (RNP) and the Brazilian Consortium. His main task is to ensure that the Brazilian project follows the guidelines of CTIC (RNP). This includes supervising the technical and scientific work of the Brazilian project team and ensuring that the objectives are met. He will synchronise on a regular basis with the PCO.

The PCO is supported by an **Administrative Manager** (AM)—Katja Böttcher (TUD-EPC)—who will be responsible for all administrative, financial and legal tasks arising in connection with the project:

* Timely collection and preparation of financial reports, including collection of financial statement, from the beneficiaries for transmission to the EC;
* Preparation and maintaining of the Consortium Agreement as well as any legal and contractual matters;
* Financial management, such as
  + Control of the project budget and preparation of the distribution of payments to the European project partners,
  + Supervision of the budget, and submission to the Management Board to any variation or modification requested by partners,
  + Providing administrative support for the project participants,
  + Checking of the individual financial statements,
  + Preparation of summary financial reports, and
  + Obtaining audit certificates.

If one or more partners are late in submitting project deliverables, the PCO may submit the other partners’ project deliverables to the EC and likewise the BCO to CTIC (RNP). Neither PCO nor BCO are entitled to act or to make legally binding declarations on behalf of any other party.

#### Management Board (MB)

The Management Board (MB) of SecureCloud is the ultimate decision-making body of the consortium and is responsible for the overall direction of the project. It consists of one representative of each European and Brazilian partner and is co-chaired by the PCO and BCO. The MB is the highest instance in our management structure and ensures that the project objectives are met and the participants adhere to the schedule. The MB decides on general contents of the project work, changes to the Annex I ‘Description of the Action’, finances, intellectual property rights and the evolution of the consortium (e.g. entry or withdrawal of partners).

In order to support the work of the MB four general meetings are planned. These are face-to-face meetings of all partners. The meetings will take place at one of the participant institutions, the location will alternate between Europe and Brazil. The first meeting (kick-off) will ensure a common understanding of the overall project goals and of the management procedures (including reporting and decision making) in particular. The next three meetings are planned to happen shortly after the milestones MS1/MS2, MS4 and MS5. Thus, these meetings will allow a broad discussion with respect to the current status of the project and any changes to the overall roadmap which might be necessary.

Besides these face-to-face meetings, the MB will hold video/telephone conferences each two months. These will serve as a platform for discussions, knowledge transfer and decision making. These regular conferences are scheduled and organised by the coordinators.

The members of the MB will stay in close contact and, if required, additional conferences will be held. In case of any problems or unforeseen circumstances, the MB will decide on necessary modifications of the work plan. For details on conflict management, see the section below.

#### Project Boards (PB)

While the Management Board takes care of the overall progress towards the envisaged project goals the Project Boards are mainly for management tasks which are specific to the European and the Brazilian projects (e.g., financial issues, reporting to the EC). Decisions made in one of the Project Boards should have only negligible influence on the other project as well as the overall results. Otherwise the decision making should be forwarded to the Management Board.

The European Project Board consists of one representative of each European partner. It will be chaired by the PCO (TUD). Its main task is to ensure that the European project follows the Horizon 2020 guidelines and that the project objectives meet the European requirements. Likewise, the Brazilian Project Board consists of one representative of each Brazilian partner. It will be chaired by the BCO (LACTEC). Its main task is to ensure that the Brazilian project follows the guidelines of CTIC (RNP) and the project objectives met the local Brazilian requirements. Both boards will have their (local) regular meetings quarterly by means of video/telephone conferences (or co-located with face-to-face meetings if applicable). Extraordinary meetings can be requested by each representative.

#### Technical Board (TB)

The research and innovation activities are arranged into 5 technical WPs, which are steered by the individual WP leaders. Each European WP Leader has a Brazilian deputy and vice versa. This approach ensures the close interaction on technical level between the European and Brazilian consortium. Together they constitute the Technical Board (TB). The TB is the supervisory body for the project execution at an operational level. The TB is responsible for the technical monitoring, direction and progress of the project and coordinates the cooperation and information flows between the WPs. It monitors the effective and efficient implementation of the project. The TB will meet together with the MB; monthly phone and video conferences are planned.

|  |  |  |
| --- | --- | --- |
| **WP** | **Leader/Deputy** | **Person** |
| 1 | TUD (leader) | Christof Fetzer |
| *LACTEC (deputy)* | *Rodrigo Riella* |
| 2 | UFCG(leader) | Andrey Brito |
| *TUD (deputy)* | *Christof Fetzer* |
| 3 | IMP (leader) | Peter Pietzuch |
| *UFCG (deputy)* | *Andrey Brito* |
| 4 | UniNE(leader) | Pascal Felber |
| *UTFPR (deputy)* | *Keiko Fonseca* |
| 5 | LACTEC(leader) | Rodrigo Riella |
| *IEC (deputy)* | *Leonid Lev* |

In detail the WP Leaders (and deputies) are responsible for:

* Preparing WP planning and coordination of tasks within their work package;
* Progressing and reporting against the work plan;
* Preparing WP meetings, as well as meeting agendas and minutes;
* Creating and updating lists of work package risks;
* Ensuring the timely and quality output from the work packages to the TB;
* Ensuring completeness of their deliverables;

Table 3.2‑2: List of WP Leaders and deputies

* Providing to contributing partners detailed technical knowledge and advice about the work area being covered by the WP tasks; and
* Providing the PMT with the information required to progress, update and maintain plans.

#### Exploitation and Innovation Manager (EIM)

Since driving innovation and coordinating exploitation is a major key success factor of the project SecureCloud will have an Exploitation and Innovation Manager (EIM)—Prof. Luigi Romano, SyncLAB. He will be the responsible person in the consortium for managing and coordinating all the innovation and exploitation related activities, with the final aim of a more effective innovation content of the project outcomes, to obtain a better commercialisation of the project results. The main activities of the EIM will be:

* Definition of indicators and/or measures to control and foster the innovation content of the progressing outcomes of the consortium partners,
* Give regular feedback on the adequacy of innovation efforts towards the exploitation of related results (in close collaboration with business development departments of industry partners and representatives from Advisory Board);
* Stimulate joint partners’ exploitation and innovation activities,
* Review and maintain partners' exploitation and IPR plans and activities,
* Organisation of continuous exchange with Advisory Board and potential customers;
* Definition of indicators to measure and control the innovation progress of the developments
* Coordination, but not deciding upon knowledge management including IPR related aspects, dissemination and exploitation of the project results.

The EIM is working closely together with the PMT. Moreover, Prof. Luigi Romano manages the project exploitation and innovation activities that are part of WP6 Dissemination, Exploitation and Communication Activities. Prof. Luigi Romano has a valuable experience in taking research ideas to the business domain. He is one of the founders of EPSILON srl (http://www.epsilonline.com), a start-up company born as a spin-off from the University of Naples Federico II. He has given several radio and TV interviews, as well as invited talks at a variety of events on exploitation-related topics. As an example, he was recently interviewed by TV journalist Cristiana Barone on the benefits of EC funding for SMEs (the interview went on air nationwide on March 4, 2015), and will be one of the panellists on research, innovation and technology transfer in European cybersecurity SMEs of the 2015 edition of the Cybersecurity & Privacy Innovation Forum (co-organized by the EC). Also importantly, he is the Innovation Manager of the SERECA project.

#### Advisory Board (AB)

The project consortium of SecureCloud works closely with an advisory board. The AB will be managed by the PCO and consulted by the MB. The AB consists of experts and representatives from different domains such as industrial partners, end users, and regulation authorities. The decision for setting up such a committee was driven by the fact that it is strived for a wide support for the innovation activities in SecureCloud by giving feedback on market needs and relevant developments. The SecureCloud project already received the commitment to participate in the advisory board from two industrial parties (Intel, SAP), a university (KTH Royal Institute of Technology, Sweden), and a public body (city hall of Curitiba, Brazil).

The AB has two important functions:

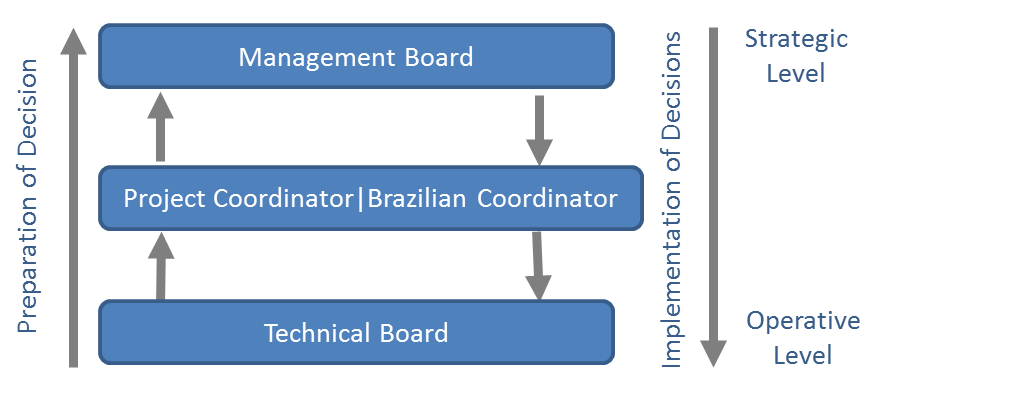
* Providing feedback on project outcome, e.g. review of intermediate results, internal reports, publications, in order to ensure that SecureCloud pursues its objectives in an adequate manner and addresses needs of relevant European industry as well as reacts on recent trends in this domain.
* Serving as dissemination channel for SecureCloud results. It is the direct way to inform potential and interested industry and businesses about the project outcomes.

In order to establish a continuous information and feedback flow between the SecureCloud consortium and the AB, two instruments are implemented:

* The AB and the project consortium meet at least twice during the project duration in conjunction with a MB Meeting but also through telephone and email exchanges on a regular basis.
* The AB has direct access to the project outcomes. It is informed on progress, intermediate results and publications. Representatives from the AB are involved in the project review process.

### Decision making and conflict resolution

Mandatory decision rules and agreements are necessary for the success of the project. The decision making process will follow the guideline to reach agreement as close as possible to the level of execution. At the task level, decisions will be taken through discussion among WP Leaders, Task Leaders and participants contributing to that particular task. If a decision impacts other WPs (second level of conflict escalation), the issue will be reported to the TB that will steered by the PCO and BCO to mediate among the WP leaders and proposes a consensual solution. If no consensus can be reached, the issue is discussed in the MB. The third level deals with strategic decisions that are taken by the MB (see Figure 3.2‐2).

The AB is advisory in nature and therefore, though it might be asked for its expertise in technical questions, it is never involved in decision making or conflict resolution.

Decision-making will be described in detail in the Consortium Agreement. In general, decisions in the MB shall be taken by consensus. If a consensus cannot be reached, decision shall be taken by simple majority of all attending representatives, where each member of a consortium body has one vote.

Figure 3.2‑2: Decision Making in SecureCloud

The presence at least of two-third of all MB members is provided, or as otherwise agreed between partners in the Consortium Agreement.

A decision gets accepted if the majority of the European partners and the majority of the Brazilian partners have voted for that decision. Otherwise, it gets rejected. If a decision gets a majority only within one group (European partners or Brazilian partners) the coordinators will try to mediate. Afterwards, a second vote will happen. If there is still no clear decision towards acceptance/rejection each of the Project Boards will decide individually on the issue according to decision making procedures of the European and Brazilian projects.

The European and Brazilian Project Boards serve only as fall back. Only if no agreement could be found in the MB both Project Boards will take the necessary decisions to ensure that the European as well as Brazilian project objectives are met as good as possible in accordance to local requirements.

### Communication strategy and reporting

Efficient communication among the European and Brazilian partners is of paramount importance for a successful execution of the project. This is why both the communication strategy and the management structure are designed to allow for efficient information exchange with equally efficient and speedy subsequent decision-making processes. Therefore any significant issues including potential problems will be raised quickly to the attention of the relevant decision-making body and will be resolved in a timely manner.

#### Decisions

All decisions will be taken either at regular or extraordinary meetings or through email and/or teleconference voting. It is essential that the partners, especially those involved in the same work packages, communicate on an almost daily basis. Therefore a list of contact persons will be created and will be maintained by the PCO and BCO telephone, e-mail, Skype, mail, and fax information. This information will be made available to all partners and maintained in a web-based platform.

#### Face-to-face communication

Regular meetings (e.g., kick-off meeting, project meetings, and the final meeting) of all partners and the funding agencies representatives will be held at least yearly during the term of the project (described in more detail in the MB section above). Additional meetings will be organised if and when required, preferably on the occasion of relevant conferences or similar events. Work package meetings will be organised as often as necessary, typically on a six-monthly basis. Bilateral meetings will take place whenever needed.

#### Electronic communication and information exchange

Day-to-day discussions and exchange of information will be done mainly via e-mail and teleconferences, but also by messaging systems such as Skype. With regard to communication with the public, potential partners and beneficiaries (e.g. potential users, policy stakeholders) of SecureCloud in the future, a **public website** will be created and maintained with the latest information on the project and relevant public documents (see section 3.2). Moreover this website will host a project internal collaboration platform which comprises web bases tools such as Wikis, blogs, revision control systems, ticket systems (e.g. for bug tracking), tools for screen sharing etc.

#### Straightforward planning and progress reports

Planningwill be performed at three levels with respect to the project goals:

* The overall project plan will be maintained by the PMT;
* The work package plans will be maintained by the WP Leaders, coordinated and communicated to the PMT on a regular basis;
* Activities within WPs will be planned by the WP Leaders in consultation with Task Leaders and involved persons where required.

During the technical project meetings the next steps of project realisation will be discussed. The TB will take operative decisions and the MB will take all strategic decisions.

Reporting to the Commission will be a task of the PMT. On a quarterly basis, WP Leaders produce short internal technical status reports describing the progress for the past period and identifying the planned work for the next period while considering any deviations from the plan and proposing corrective measures. These reports are delivered to the PMT. The PMT will collate and approve the final internal reports for distribution.

Additionally, bi-annually internal financial reports will be prepared by each partner allowing the PMT to monitor actual costs and spent effort but also to detect and prevent possible financial errors.

All deliverables and reports are to be distributed electronically and made available after internal review and quality assurance (see Section 3.2.4) to all partners via the SecureCloud collaboration infrastructure. The PCO and BCO in agreement with the project consortium control the distribution of deliverables, for internal use and to external parties. For public dissemination the SecureCloud Website will be used (WP6). The PCO is in charge of sending periodic and final financial and technical reports to the European Commission, with the full support from all partners. Likewise the BCO is responsible for reporting towards the CTIC (RNP).

### Quality assurance and risk management

The scheduling of milestones (see Table 3.2-2) and deliverables (see Table 3.1-3) will allow for monitoring the project evolution, measuring the advancements made by qualitative and quantitative evaluations, (re)defining priorities and optimizing project progress by corrective measures.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **MS no.** | **Milestone name** | **Related WPs** | **Estimated date** | **Means of verification** |
| M1 | Initial requirements and specification | WP1 | M09 | This milestone will be met by providing the initial set of requirements and uses cases as well as a comprehensive architec­ture description and specifi­cation of the APIs between all SecureCloud compo­nents |
| M2 | Interface level component integration | WPs 1, 2, 3, 4 | M13 | This milestone will be met by assuring that different components of the SecureCloud platform can com­muni­cate between each other (interface level). |
| M3 | Functional component integration & first set of applications | WPs 1, 2, 3, 4, 5 | M18 | This milestone will be met by assuring that different functional components can interoperate. Moreover a first set of applications that process data from smart grids in the cloud was evaluated successfully. |
| M4 | Prototype | WPs 1, 2, 3, 4, 5 | M25 | The SecureCloud prototype has reached a level of maturity to allow running the full-fledged use case applications, even though some design aspects are not finalised yet. The Demonstrator for the end-to-end secure and privacy-friendly smart meter data processing was evaluated successfully. Further, there is an updated requirements and design document. |
| M5 | Final SecureCloud platform | WPs 1, 2, 3, 4, 5 | M33 | All SecureCloud components are released and evaluated. The final architecture and all the interfaces are well defined and described. The complete SecureCloud platform, including the two use cases, is integrated and validated.  Only minor open issues remain to be solved. |

Table 3.2‑3: Scheduling of milestones

Quality control and assurance will allow maximum flexibility while maintaining a clear distinction of roles and responsibilities of all partners involved. To this end, the project will establish appropriate mechanisms and procedures, involving all partners.

An internal Quality Assurance Planwill be set up for the consortium identifying an unambiguous and appropriate workflow between consortium partners and the various roles designed for the project. The goal is to ensure the detection of errors and deviations as early as possible in the project’s life cycle and to provide measures how to handle such issues. This will enable the consortium to apply systematically corrective actions or contingency plans, if necessary.

Quality control and assurancewill be the basis of self-assessment for the project and will control the input and output of, as well as the interactions between, all WPs within the project. The purpose of the quality assurance activities in SecureCloud is to ensure that the project fulfils its objectives also in terms of the quality (technical, formal) of the deliverables, internal reports and publications. In addition to that each involved person has the main responsibility for the quality of the own work, the document review procedures have been defined and deployed to support that work.

The SecureCloud project is aiming at a high level of quality of its documents and other deliverables to fulfil the goals and milestone of the project, e.g. by partner peer-review and feedback by the AB.

Accordingly the project will implement a formal review procedure to ensure continuous quality of it documents and other deliverables, e.g. by having draft deliverables available a few weeks before the deliverable’s deadline for internal review by the consortium and the AB. This procedure is designed to enable the project team to both monitor the quality of documents and other deliverables while being developed, and to formally review their content upon finalization. The approval process will be determined in the Consortium Agreement.

An appropriate risk assessment and managementis important to ensure the timely fulfilment of SecureCloud’s challenging objectives. The GA will ensure that all necessary actions will be undertaken to minimize risks and to drive all necessary counter measures. The risks listed below (see Table 3.2-3) are a snap-shot of the risks we can already define and assess at the time of proposal writing. A detailed risk review will be performed at the start of the project.

Project risks are susceptible to change and as such will be reviewed continuously at the WP technical meetings and bi-annually at the full consortium meetings. It is the role of the project management in WP1 to maintain an up-to-date risk table and to modify risk levels as appropriate in consultation with the TM.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Description of risk** | **WP(s) involved** | **Proba-bility**[[49]](#footnote-50) | **Impact2** | **Proposed risk‐mitigation measures** |
| Defaulting partner | All | L | H | The PMT has to decide how the contract obligations will be fulfilled by the consortium in accordance with the CA |
| A key member of staff (WP-leader, project coordinator, etc.) leaves the project | All | L | H | The project management will minimize this risk by setting up regular conference calls and ad-hoc meetings to establish and motivate communication with partners. The GA will be used for the resolution of problems and conflicts. In case a partner would indeed leave the consortium, we have sufficient expertise in the consortium to assign—if needed—the affected tasks to the other partners in the consortium. |
| The scope of the project is too ambitious for the given person months. | All | M | M | The project consortium will ensure through proper requirement analysis and planning that the objectives can be achieved. A state of the art software process management approach will be used to execute our plan and to balance scope, quality, resource usage and timeliness. |
| Project costs in a WP are in danger of exceeding the amounts foreseen in the budget. | All | M | L | Project management to establish monitoring of resource consumption and comes up with plans to achieve our goals in a more resource efficient manner. |
| Lack of communication or consensus within the consortium | All | L | H | Within the proposal management procedures have been defined for enabling effective decision making. The PC and the members of the GA have the necessary skills to resolve such conflicts by adequate negotiation. Additionally it is planned to keep close contact within the consortium by regular telephone conferences and virtual meetings. |
| A deliverable is delayed | WP1 | M | H | The project management will monitor continuously the progress of work in accordance with defined work plans by means of quarterly scientific reports delivered to the coordinator by the WP Leaders. If needed, redistributing of resources and manpower or alternative approaches will be considered to reach deadlines. |
| Dissemination of the  project results is not sufficient to create  impact | WPs 2-5 | L | M | The consortium is strongly determined to create sustaining impact, and the partners have substantial experience in the international R&D business; a dedicated WP for dissemination, exploitation and communication strategies under the lead of the Exploitation and Innovation Manager will plan and execute this. |
| Intel SGX  not available. | WPs 2-5 | M | L | If no Intel SGX Hardware is available for the project, we will also exploit alternative services architectures that consider only secure computing technologies based on TPMs to develop secure services. Moreover we will elaborate on using a software-only emulator of Intel SGX or a similar technology. |
| Our contributions to OpenStack are not accepted into core services. | WPs 2-3 | M | L | The OpenStack ecosystem is composed of a few main projects and a multitude of accessory projects with more restricted goals. Some of the services we will develop are likely to be implemented in the main projects (e.g., being able to consider the support for security features during scheduling for resource provisioning) and some, more innovative, may be first redirected to incubated projects. In both cases, an interested user or cloud provider will still have access to the technology. |
| Big-data applications developed to validate the cloud infrastructure do not scale when using secure containers. | WPs 2-5 | L | L | Services can be architected and application programming models and patterns proposed to minimize the portion of the application that needs to run in the secure container. A trade-off between security, performance and programming flexibility will then be evaluated together with the industrial partners and the scientific community. |
| The development of reusable micro-services takes longer than anticipated, delaying the development of the use case demonstrators. | WPs 3,4,5 | L | H | If the development of a given micro-service becomes more challenging than anticipated, the task in WP3 will deliver an initial dummy version that may not be secure, but will permit parallel development in WP4 and WP5. |
| The definition of the framework API for secure micro-services may be challenging when trying to guarantee security properties. | WP3 | M | M | As evidenced by prior work that proposes hardened systems call and hypervisor APIs, the development of rich yet secure APIs is difficult. We hope to mitigate this risk by relying heavily on prior approaches that faced similar problems such as the work on secure library operating systems that execute using trusted hardware. |
| Incorrect or incomplete  identification of strategies and policies for Securecloud platform | WPs 1-4 | M | M | Tests and case studies. Factory trials. Communication with industry advisory board members. |
| Integration problems, continuous cooperation and communication among teams. | WP7 | M | M | Frequent progress reviews will allow the Project  Coordinator and the Project Coordinator Team to track project progress against time and costs, identify in advance possible criticalities and evaluate corrective actions such as re-scheduling and re-allocation of resources. |
| Weak or insufficient partners contribution  (technical and managerial) | WP7 | M | M | Balanced composition of consortium will avoid gaps in technical skills or management.  Tasks/responsibilities can to a certain extent be  assumed by other member(s) |
| Disclosure of confidential information of partner. | WP7 | M | M | Confidentiality will be signed |

Table 3.2‑4: Estimated risks and mitigation plans

## Consortium as a whole

The two main objectives of SecureCloud are (1) the **development of a secure cloud platform** and (2) to **evaluate the platform with** the help of privacy- and security-enhanced **big data demonstrators** in the area of smart grid including smart metering.

To achieve the targeted objectives, SecureCloud requires partners with a broad range of backgrounds, competences, and assets. The academic partners have previously demonstrated scientific and research excellence, while the industrial partners provide the practical skills, experience, and infrastructure for data acquisition and evaluation. The areas of competence that are important for SecureCloud are on the one hand related to cloud infrastructures, IT security and privacy, and big data processing. On the other hand, the practical big data use cases require knowledge about smart grids, smart metering technologies, procedures, infrastructures, operations, and testbeds. The consortium, consequently, consists of a well-balanced mixture of research and industrial partners covering all the required skills and fields of expertise, with minimum overlap. The participating individuals represent a good spread of professional competences in project-critical technical and non-technical areas. The consortium thus brings together a number of world leading research groups with high visibility in their respective fields.

The consortium brings together 14 organisations in total (7 from Europe, 7 from Brazil), including 6 universities (3 from Europe, 3 from Brazil), 2 Brazilian research centres, and 6 industrial partners (4 from Europe, 2 from Brazil).

|  |  |
| --- | --- |
|  |  |
| Figure 3.3‑1: Consortium as a whole (European and Brazilian consortium) | |

As shown in Table 3.3-1, the Brazilian partners will concentrate their effort in the development of the demonstrators in the area of smart grid and smart metering. The European partners will develop the enabling technologies in terms of the secure cloud infrastructure and big data processing technologies.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Europe | | Brazil | |
|  | **Enabling tech.** | **Application** | **Enabling tech.** | **Application** |
| Universities | TUD  IMP  UniNE |  | UFCG | UTFPR  UNIFEI |
| Research Centres |  |  |  | LACTEC  INMETRO |
| Industrial Partner | Chocolate Cloud  CloudSigma  SYNC | IEC |  | COPEL  CAS |

Table 3.3‑1: Distribution of partners according to location, type of organisation and field of expertise[[50]](#footnote-51)

The development, implementation and evaluation of the enabling technologies of the SecureCloud platform will be mainly shared among TUD, IMP, UniNE, UFCG, Chocolate Cloud, CloudSigma, and SYNC. CloudSigma, as a large European cloud provider, will steer the gathering of the SecureCloud requirements. CloudSigma’s experience with Cloud customers (end users), and as a Cloud provider will provide valuable input from two distinct perspectives. Moreover, CloudSigma will host and maintain hardware to implement (parts of) the SecureCloud platform as well as for tests and evaluation under realistic conditions. Finally, CloudSigma will contribute its own cloud stack as one foundation for the SecureCloud platform.

Besides CloudSigma, Synclab will contribute to the requirements analysis and to the use-case development. Synclab, a company developing big data analytics software, will take the point of view of a Cloud user, to ensure that the SecureCloud platform meets all the requirements necessary to run state-of-the-art big data analytics software.

TUD, IMP, UniNE, and UFCG, have a strong track record in outstanding research in the area of large-scale distributed systems as well as security and privacy. They will jointly create the overall architecture of the SecureCloud platform. TUD will concentrate on the development of secure containers (WP2). IMP will focus on the development of a novel set of secure micro-services to be executed within the secure containers (WP3). UniNE’s main contribution will be the development of a generic mechanisms for big data processing utilising the secure micro-services (WP4). These big data processing mechanisms will be used by the application level demonstrators. Besides secure and efficient processing of big data, the secure storage of large amounts of data will be another service provided by the SecureCloud platform. The main responsible partner for this task will be Chocolate Cloud due to their expert knowledge. Chocolate Cloud will contribute their existing secure storage solution to the SecureCloud platform. UFCG, besides their general experience with Cloud computing and the development of related enabling technologies, is particularly knowledgeable about the OpenStack cloud management software. More specific, UFCG is the university with the most contributions to OpenStack (considering lines of code, see www.stackalytics.com) and will therefore help with the implementation of basic services to use secure containers as well as with the integration of the applications in a cloud infrastructure and their validation.

Regarding the smart meter demonstrator (Task 5.1, Task 5.3) the involved partners are: COPEL, CAS, LACTEC, UNIFEI, and INMETRO. COPEL as a large utility will contribute to the requirements collection from an end-users point-of-view and will provide access to real-world Smart Meter measurements. CAS, as a major supplier of meter data-management and analytics software, will contribute to the requirements collection, to the implementation for processing smart meter data, and will help with the evaluation of the developed solution. LACTEC, being involved in many smart meter projects, will contribute smart meter hard- and software, which can be adapted according to the project needs. LACTEC will also develop and implement these enhancements. UNIFEI, being an expert in the area of embedded systems, especially embedded systems security, will help in the development of a secure smart meter. Finally, INMETRO, being the Federal Institute responsible for all aspects related to metrology in Brazil (Regulation, Standards, Conformity Assessment etc.), will help to collect the requirements from a regulatory point of view and develop an integrated solution, which complies with all the relevant regulations. Moreover, INMETRO will feedback the demonstrator results into national and international standardisation and regulation bodies.

The second demonstrator (Task 5.4) is about quality of service of the smart grid including fault detection and fault recovery. The main partners involved are: COPEL, UNIFEI, UTFPR, and IEC. *COPEL*, being again the end-user of the solution developed, will contribute their requirements and give feedback regarding the achieved results. UNIFEI will contribute their expertise in the area of power systems regarding monitoring, fault detection, fault classification and recovering. UTFPR’s knowledge and expertise in the area of distributed real-time systems will ensure that the solutions developed meet the hard real-time requirements of the (smart) power grid. Finally, IEC, being an expert in test and validation and having a large smart grid testbed, will evaluate the demonstrator under close to real-world conditions.

|  |  |
| --- | --- |
| Required skills, competences and experienced | SecureCloud partner |
| Use-cases and requirements | Synclab, CloudSigma, COPEL, CAS |
| Development of large-scale distributed systems | TUD, IMP, UniNE, UFCG |
| Secure containers (TPM, Intel SGX) | TUD, IMP |
| Micro-service paradigm | IMP |
| Secure storage | Chocolate Cloud |
| Efficient and secure communication (network) | TUD, Chocolate Cloud |
| Big data processing | UniNE, IMP |
| Cloud software stacks like OpenStack | CloudSigma, UFCG |
| Cloud infrastructure | CloudSigma |
| Privacy (especially in Smart Meter applications) | TUD |
| Real-time processing | UTFPR |
| Regulations | INMETRO |
| Smart meter test data | COPEL, IEC |
| Smart meter hardware and software | LACTEC, CAS |
| Embedded systems security | UNIFEI |
| Fault detection in power systems | UNIFEI |
| Smart grid testbed | IEC |
| Test and Validation | IEC |
| Dissemination, Training, Standardisation | TUD, UniNE, IMP, UFCG, UTFPR, UNIFEI, LACTEC, INMETRO, Synclab |
| Management of international cooperation projects (administrative, financial, quality assurance) | TUD, LACTEC |

Table 3.3‑2: Required competences and related partners

Further to the technical skills mentioned above (cf. Table 3.3-2), SecureCloud also needs to choose partners capable of working in diverse international teams and with a track record of delivering in complex international collaborative projects. These skills are justified by the various successful European (e.g. FP7) and international projects of each project partner. Moreover, certain subsets of project partners have already successfully worked together in different projects: TUD, UFCG, UTFPR, UNIFEI, LACTEC, and INMETRO have cooperated in the TruEGrid project. LACTEC, CSA, and COPEL cooperated in the Smart Grid Paraná project. TUD and UniNE cooperate in the EU FP7 project LEADS. TUD and IMP currently cooperate in the H2020 SeReCa on the use of trusted hardware features (including Intel SGX) to create the next generation of secure reactive web application. Their obtained expertise on the SGX technology will be invaluable to SecureCloud.

To summarize, the SecureCloud consortium has the complete knowledge and the necessary capabilities to develop, implement and evaluate the SecureCloud platform as well as the demonstrators.

## Resources to be committed

The SecureCloud project estimates total project costs amounting to 2,285,378 EUR for the European consortium. The total requested funding amounts to 1,499,628 EUR resulting from the fact that our Swiss partners UniNE and CS will be financed by the Swiss State Secretariat for Education, Research and Innovation (SERI). The budget is mainly based on personnel costs (271 person-months for the European project partners, corresponding to 87% of total direct costs), travel cost (8.4%), costs for durable equipment (2.9%), and other direct costs including audit costs for partners TUD, IMP, UniNE (1.7%), see Figure 3.4-1.

Figure 3.4-2 illustrates the estimated budget distribution per type of **participating organization**, which stresses the active participation of industry and involved SMEs.

|  |  |
| --- | --- |
|  |  |
| Figure 3.4‑1: Distribution of costs among European partners | Figure 3.4‑2: Estimated budget distribution between participating European organization types |

### Summary of staff effort

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **WP1** | **WP2** | **WP3** | **WP4** | **WP5** | **WP6** | **WP7** | **Total PMs** |
| **1 TUD** | **13** | 13 | 20 | 2 | 4 | 2 | **14** | **68** |
| **2 IMP** | 1 | 9 | **28** | 16 | 1 | 1 |  | **56** |
| **3 UniNE** | 1 | 7 | 10 | **33** | 1 | 1 | 1 | **54** |
| **4 CC** | 2 |  |  | 22 | 2 | 2 |  | **28** |
| **5 SYNC** | 12 | 2 |  |  | 17 | **3** | 1 | **35** |
| **6 IEC** | 2 |  |  |  | 5 | 1 | 1 | **9** |
| **7 CS** | 5 | 8 |  |  | 4 | 4 |  | **21** |
| **8 LACTEC** | 3 |  |  |  | **32** | 4 | **18** | **57** |
| **9 UFCG** | 9 | **62** |  |  | 12 | 2 |  | **85** |
| **10 UTFPR** | 3 |  |  | 6 | 31 |  |  | **40** |
| **11 UNIFEI** | 3 |  |  |  | 22 |  |  | **25** |
| **12 COPEL** | 3 |  |  |  | 2,5 |  |  | **5,5** |
| **13 CAS** | 3 |  |  |  | 27,5 |  |  | **30,5** |
| **14 INM** | 3 |  |  |  | 24 |  |  | **27** |
| **Total PMs** | **63** | **101** | **58** | **79** | **185** | **20** | **35** | **541** |

Table 3.4‑1: Summary of staff effort

Figures 3.4-3 and 3.4-4 illustrate the effort distribution among the participating countries as well as among industry and academia.

|  |  |
| --- | --- |
|  |  |
| Figure 3.4‑3: Planned effort distribution among participating countries | Figure 3.4‑4: Planned effort distribution among organisation types and WPs |

### Other direct cost’ items (travel, equipment, other goods and services)

In the tables below the sum of the costs for’ travel’, ‘equipment’, and ‘goods and services’ for partners IEC and CS are detailed as these costs exceed 15% of the personnel costs (cf. budget table in Section 3 of the proposal administrative forms).

|  |  |  |
| --- | --- | --- |
| **6 - IEC** | **Cost (€)** | **Justification** |
| **Travel** | 17,000 | Participation in four project meetings, two review meetings with European Commission, several dissemination events, such as conferences and workshops to promote results of SecureCloud and travel costs related to the implementation of the project |
| **Total** | 17,000 |  |

|  |  |  |
| --- | --- | --- |
| **7 - CS** | **Cost (€)** | **Justification** |
| **Travel** | 6,000 | Travel costs related to the implementation of the project |
| **Equipment** | 45,000 | In order to facilitate the goals of SecureCloud, the necessary hardware (namely Intel SGX equipped servers) will need to be procured, shipped, installed and maintained in one of CS’ European data centres. |
| **Other direct costs** | 22,000 | Hosting of the aforementioned hardware over the course of the project based on powering and hosting of two Intel SGX hosts and will be paid to the data center provider. |
| **Total** | 73,000 |  |

1. See https://dockerhub.com [↑](#footnote-ref-2)
2. Of course, the security of the hypervisor, operating system and the cloud must not be neglected since successful attacks can lead to the unavailability of hosts and hence, to the unavailability of some application components. [↑](#footnote-ref-3)
3. **SCONE: Secure Linux Containers with Intel SGX** (Sergei Arnautov, Bohdan Trach, Franz Gregor, Thomas Knauth, André Martin, Christian Priebe, Joshua Lind, Divya Muthukumaran, Daniel O'Keeffe, Mark L Stillwell, David Goltzsche, Dave Eyers, Rüdiger Kapitza, Peter Pietzuch, Christof Fetzer), USENIX, 2016. [↑](#footnote-ref-4)
4. http://www.t-mobile.com/landing/experian-data-breach.html [↑](#footnote-ref-5)
5. https://software.intel.com/en-us/sgx [↑](#footnote-ref-6)
6. http://www.gartner.com/newsroom/id/3188817 [↑](#footnote-ref-7)
7. https://en.wikipedia.org/wiki/Heartbleed [↑](#footnote-ref-8)
8. see https://hub.docker.com/explore/?page=1 [↑](#footnote-ref-9)
9. Within the SERECA project, there is already support for JamVM an small Java virtual machine. Which would be out backup in case OpenJDK will not be supported after all. [↑](#footnote-ref-10)
10. https://www.mono-project.com [↑](#footnote-ref-11)
11. http://www.exus.co.uk/en/products/debt-collection-software-suite [↑](#footnote-ref-12)
12. http://www.zdnet.com/article/us-strikes-back-in-microsoft-email-warrant-case/ [↑](#footnote-ref-13)
13. http://www.synclab.it/prodotti/streamlog/ [↑](#footnote-ref-14)
14. 2015- Global Megatrends in cyber security , Ponemon institute, published 02/2015 [↑](#footnote-ref-15)
15. In the rest of this proposal we will use the acronym SGX (Software Guard Extensions) to refer to the needed security extensions of a given processor. Nevertheless, we will develop our solution to be as flexible as possible so that it can be adapted to any processor which offers the need security functionality—not just Intel processors. [↑](#footnote-ref-16)
16. http://www.theregister.co.uk/2014/04/09/heartbleed\_explained/ [↑](#footnote-ref-17)
17. this is the usable size of the EPC (extended page cache) of current generation SGX implementations. [↑](#footnote-ref-18)
18. http://zerovm.org/ and http://zerg.erlangonxen.org/ [↑](#footnote-ref-19)
19. http://www.serecaproject.eu [↑](#footnote-ref-20)
20. http://www.a4cloud.eu/ [↑](#footnote-ref-21)
21. http://contrail-project.eu/ [↑](#footnote-ref-22)
22. http://cloudcert.european-project.eu/index.php?lang=en [↑](#footnote-ref-23)
23. http://www.cumulus-project.eu/ [↑](#footnote-ref-24)
24. http://ict-passive.eu/ [↑](#footnote-ref-25)
25. http://www.practice-project.eu/ [↑](#footnote-ref-26)
26. http://www.seccrit.eu/ [↑](#footnote-ref-27)
27. http://www.secfunet.eu/ [↑](#footnote-ref-28)
28. http://www.tclouds-project.eu/ [↑](#footnote-ref-29)
29. http://www.trescca.eu/ [↑](#footnote-ref-30)
30. Cisco Global Cloud Index: Forecast and Methodology, 2013–2018: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud\_Index\_White\_Paper.pdf [↑](#footnote-ref-31)
31. http://news.investors.com/technology/011615-735080-amazon-aws-leads-in-cloud-msft-googl-crm-rising.htm [↑](#footnote-ref-32)
32. Network World’s “2015 State of the Network Study, Technology Adoption Trends & Their Impact on the Network”: https://www.scribd.com/document\_downloads/253406492?extension=pdf&from=embed&source=embed [↑](#footnote-ref-33)
33. http://www.rackspace.co.uk/sites/default/files/UnlockedNov2014\_TheRoleOfCloudInITModernisation\_Ovum.pdf [↑](#footnote-ref-34)
34. Forrester Forecast: http://www.zdnet.com/article/enterprise-software-spend-to-reach-620-billion-in-2015-forrester/ [↑](#footnote-ref-35)
35. http://www.skyhighnetworks.com/cloud-report/ [↑](#footnote-ref-36)
36. Symantec ® Applied Research. Symantec 2010 Critical Infrastructure Protection Study (Global Results), October 2010. [↑](#footnote-ref-37)
37. Symantec® Intelligence Quarterly Report: October-December, 2010, “Targeted Attacks on Critical Infrastructures.” [↑](#footnote-ref-38)
38. McAfee ® White Paper, Global Energy Cyberattacks: “Night Dragon”, Foundstoner Professional Services and McAfee Labs, (February 10, 2011). [↑](#footnote-ref-39)
39. Stewart Baker, Shaun Waterman, George Ivanov, “In the Crossfire: Critical Infrastructure in the Age of Cyber War”, McAffee Labs, 2010. [↑](#footnote-ref-40)
40. https://cloudharmony.com/status-1year-of-compute-and-paas-and-storage-group-by-regions [↑](#footnote-ref-41)
41. http://www.chefuturo.it/2015/04/e-health-la-salute-diventa-digitale-presto-gli-smartphone-sapranno-tutto-di-noi-e-ci-aiuteranno-a-curarci-prevenendo-le-malattie-gravi/ [↑](#footnote-ref-42)
42. 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2013. [↑](#footnote-ref-43)
43. Alert Logic CLOUD SECURITY REPORT – SPRING 2014. [↑](#footnote-ref-44)
44. P. Mell and T. Grance, “The NIST Definition of Cloud Computing”, NIST Special Publication 800-145, September 2011. [↑](#footnote-ref-45)
45. F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, “NIST Cloud Computing Reference Architecture”, NIST Special Publication 500-292, September 2011. [↑](#footnote-ref-46)
46. L. Badger, T. Grance, R. Patt-Corner, and J. Voas, “Cloud Computing Synopsis and Recommendations”, NIST Special Publication 800-146, May 2012. [↑](#footnote-ref-47)
47. Technical Requirements for Supporting the Intercloud Networking, GICTF White Paper 2012-1, www.gictf.jp/doc/GICTF\_NWSWG-WhitePaper\_e\_20120420.pdf. [↑](#footnote-ref-48)
48. Intercloud Interface Specification Draft (Cloud Resource Data Model), GICTF White Paper 2012-2, May 2012, http://www.gictf.jp/doc/GICTF\_CloudIF\_ResourceDataModel\_WhitePaper\_e\_20120515.pdf [↑](#footnote-ref-49)
49. **L** = Low, **M** = Medium, **H = H**igh [↑](#footnote-ref-50)
50. In the table the term “Enabling technologies” refers to the basic building blocks necessary for implementing the secure Cloud platform as well as enabling technologies in the area of big data processing utilising the secure cloud platform. The term “Application” refers to the adaption of these enabling technologies for the uses-cases and demonstrators in the area of smart grid and smart metering as outlined in WP5. [↑](#footnote-ref-51)