ACSmI: A solution to address the challenges of Cloud services federation and monitoring towards the Cloud Continuum.

Abstract

The evolution of cloud computing has changed the way in which Cloud Service Providers offer their services and how Cloud Customers consume them, moving towards the usage of multiple Cloud Services, in what is called multi-cloud. Multi-cloud is gaining interest by the expansion of IoT, edge and the Cloud Continuum where distributed Cloud federation models are necessary for effective application deployment and operation.

This work presents ACSmI, Advanced Cloud Service Meta-intermediator, a solution that implements a Cloud federation, supporting the seamless brokerage of Cloud Services. Technical details addressing the discovered shortcomings are presented, including a proof of concept built on JHipster, Java, InfluxD, Telegraf and Grafana. ACsmI contributes to relevant elements of the European Gaia-X initiative, specifically to the federated catalogue, continuous monitoring, and certification of services. The experiments show that proposed solution effectively saves up to 75% of the DevOps teams' effort to discover, contract and monitor cloud services.

Key words: Cloud Service Broker, Cloud Services Federation, Cloud services Brokerage, Cloud Services intermediation, Hybrid Cloud, Cloud Service monitoring, Cloud Services intermediation, Multi-Cloud, DevOps, Cloud Service Level Agreement, Cloud Service Discovery, Multi cloud service management, Cloud Continuum

Abbreviations:
CB: Cloud Broker
CP: Cloud Provider
CSLA: Cloud Service Level Agreement
CSP: Cloud Service Provider
DPO: Data Protection Officer
EU: European Union
KF: Key Functionality
NFR: Non-Functional Requirement
PC: Personal Computing
TRL: Technology Readiness Level
SLA: Service Level Agreement
SLO: Service Level Objective
SOA: Software Oriented Architectures

1 Introduction

In the past years the paradigm shift from PC-centric computing to cloud computing has led into the emergence of several Cloud Services and providers. Initially, Cloud Services were offered as third-party computational capacities but now a days the offer has become more and more functional diverse, context specific and technology driven. Following this transition, Cloud services users' consumption of such services has evolved too, from one single Cloud Service type, offered by one provider to the usage of multiple Cloud Services, in what is called a Multi-Cloud approach.

Multi-cloud is defined as the serial or simultaneous use of services from diverse providers to execute an application (Petcu, 2013). At business level, Hybrid Cloud is the term commonly used. Gartner (Mazzucca and Ed, 2015) defines hybrid cloud as the coordinated use of cloud services across isolation and provider boundaries among public, private and community service providers, or between internal and external cloud services. Several scenarios demonstrate these serial or simultaneous interactions among hybrid heterogeneous private and public clouds and across all cloud layers (IaaS/PaaS/SaaS) (ETSI, 2013). Therefore, Multi-Cloud is getting more and more interest as microservices-based software applications are increasingly getting popular fostering flexibility for the developers to build applications for distributed complex environments.

Microservice architectures have evolved from the SOA concept, improving issues and challenges in terms of applications build and deployment when the size of the application becomes large and distributed (Jambunathan and Y., 2016). Microservices architectures provide isolated, loosely-coupled unit of development that works on a single concern. This independency makes them the best candidate to profit from the advantages of heterogeneous Hybrid Cloud scenarios. Each application component (or microservice) can be deployed independently, considering its specific deployment needs or desired non-functional requirements (NFR) such as location, cost, performance, etc. Specially for critical infrastructures and applications where the fulfillment of the SLAs is crucial, the possibility of selecting different types of services with different characteristics and SLOs optimized for each component incorporates relevant benefits as no NFR needs to be favored at expense of other. This new paradigm, where a single application is deployed over an ecosystem of heterogeneous and distributed cloud resources encompasses new needs in terms of management, governance, monitoring, or SLA assessment.

While the research community has focused the effort to advance in the way the software applications can be de-couple with the aforementioned micro-services based architectures and the enablers that support the operation of this kind of newly distributed applications (i.e. containerization, server-less computing, etc.) a few research initiatives have been concentrated on the management of federated, interoperable, self-monitored, and legal compliant ecosystem of cloud services from a holistic point of view, not only focusing in a single step of the Cloud Service Lifecycle, like for example the operation and deployment of the physical resources (Tordsson et al., 2012) (Michon et al., 2017).

In addition, intermediates layers to govern the complex ecosystem of Cloud Services are becoming more and more relevant as the next generation of Cloud environments emerges following the Cloud Continuum paradigm. The new Computing Continuum can be defined as a heterogeneous environment based on the decentralization and federation of diverse computing entities and resource typologies (Balouek-Thomert et al., 2019). Besides the traditional Cloud Computing services, Fog and Edge Computing services are to be part of this Cloud Continuum. To this end the support of Multi-Cloud and computing federation models is required so that diverse, decentralized and autonomic management and hybrid computing models can be implemented. The brokerage of multiple Cloud services can provide flexible means for assembling such heterogeneous Cloud-based elements in support of the Cloud Computing Continuum.

That leads to questions about how to make those heterogenous services work together, or how to unify all the efforts so maximum effectiveness and efficiency can be obtained out of the existing computing services. This is when a Cloud Service

Broker (CSB) comes into play. Their goal is to integrate or aggregate services, to enhance their security, or to do anything which adds a significant layer of value (i.e. capabilities) to the original Cloud services being offered (Alonso et al., 2017a).
Existing cloud services shall be made available dynamically, broadly and cross border, so that software providers can re-use and combine cloud services, assembling a dynamic and re-configurable network of interoperable, legal compliant, quality assessed (against SLAs) single and composite cloud services. To this extent, a viable intermediator and federator of Cloud Services Broker (Alonso et al., 2017a) can make it less expensive, easier, safer (also in legal terms), interoperable and more productive for companies to discover, aggregate, consume and extend Cloud services, particularly when they span multiple, diverse Cloud services providers in different European Member States.
This article presents a solution for Cloud Services Brokerage and Federation, ACSmI, Advanced Cloud Service Meta-intermediator (Figure 1). The paper is organized as follows. Section 2 analyses the related work introducing the challenges in Cloud Services Brokering as well as discussing existing solutions following a multi-dimensional approach and introduces the initial functional description of the proposed ACSmI solution. Section 3 includes the detailed technical design of the Cloud Service intermediator and all the subcomponents. Section 4 shows the experimental results accompanied by discussion. Section 5 summarizes the study contributions and highlights the future work directions.

2 Related work

2.1 Motivation and problem statement

As previously introduced, enabling the complex ecosystem of distributed Cloud Services to support the Cloud Continuum still lays down into several challenges for both users and providers.
First (Nizamani, 2012) and then Fortis (Fortiş et al., 2015) discussed key challenges faced by the users in moving their data/services to Cloud platforms including:

- Choosing the right provider specially for concrete needs such as regulation compliance.
- Service management, including the ability to discover, contract and operate them.
- Security and Privacy issues.
- Trustworthiness of CSPs.
- Dealing with vendor lock-in.
- Support and reliability related to liability of the cloud provider in case of SLA or QoS breaches.

From the provider's perspective, there are many challenges to be addressed being the most relevant ones (Neelakanta, 2012):

- Understanding the market, the competitors in the domain, the user preferences for various features such as security and trust requirements.
- Adapting to the market: Current Cloud platforms follow a fixed price per resource for their products and services with some small exceptions like Amazon spot pricing (Jurg van and Flavia, 2011), therefore more dynamic pricing strategies are required to attract more customers.

Considering the scientific community, researchers (Elhabbash et al., 2019) (Ibarra et al., 2016), (Juncal Alonso et al., 2019) , (Zhou et al., 2019), extracted similar conclusions from the analysis of existing Cloud Services intermediation approaches: customer assistance is not addressed as the user perspective of the Cloud Brokerage is not tackled; Complex services bidding is still a challenge limited to very few restricted characteristics of the services mainly related with the low level interoperability of the resources and not expanding to other high level layers such as the common monitoring ability or multi-contracting capability; Standards or common languages for services descriptions are missing, and the majority of works rely on simulations for verifying their solutions.

At policy level, the need of specific solutions for Cloud Services Federation is also considered as a key research objective. To this respect, the European Data Strategy released in February 2020 (European Commission, 2020) outlines a strategy for policy measures and investments to enable the data economy in Europe. Among the different problems identified in that communication the adoption of cloud is mentioned, both from the consumer and provider side. These problems include compliance with data protection regulation, multi-cloud interoperability, data portability, and the lack of a European cloud and data infrastructure. One of the four pillars upon which the data strategy is built is the proposal by the EC to create a "*a cloud services marketplace for EU users from the private and public sector [...] by Q4 2022*" where "*potential users (in particular the public sector and SMEs) [are] in the position to select cloud processing, software and platform service offerings that comply with a number of requirements in areas like data protection, security, data portability, energy efficiency and market practice*". The analysis of the presented situation enabled us (Alonso et al., 2017a) (Alonso et al., 2019a) (Juncal Alonso et al., 2019) to group the needs and propose the challenges (CH) that organizations using multi-Cloud Computing will address in the next years:

1. Governance (CH1): Ensuring that services deployed in the cloud are protected is critical. Sharing can create leaks that cannot be tolerated. Fostering strong governance programs in place will protect enterprises and their data.
2. Risk tolerance (CH2). Every enterprise should assess their tolerance for pitfalls such as lost data and application outages. As Information as a Service and Integration as a Service evolve, enterprises will see risks reduced.
3. Regulations (CH3). Lobbying for regulations and standards are predicted to be a key step to ensure cloud integration.
4. Cross border interoperability (CH4): Means to support cross border interoperability need to be put in place such as intelligent discovery, context-aware service management and fluid service integration, assuring data portability in such a federated ecosystem, while guaranteeing proper identity propagation with service-specific granularity level of information.
5. Matching customer requirements with cloud service specifications (CH5): customers in any EU country should be provided with a guarantee of security, legislation awareness and other non-functional requirements when using any cloud service within heterogeneous environment. This implies that the selected service offerings must match with all functional and non-functional requirements coming from the customers.
6. Legislation compliance, defining means of assuring service compliance with legislation of EU countries (CH6): a service is legislation aware when the services are constrained by legal requirements, such as data privacy, data protection, data security and data location. A big challenge in this concern is to develop the methods and interfaces for ensuring legislation compliance and easy legislation change propagation through composite services in a legislation heterogeneous environment.
7. Cloud Service SLA assessment and monitoring (CH7): monitor and control the diverse properties of utilized services, composite or stand-alone, at real-time, while also being able to provide all the critical information for the appropriate reactions when necessary, especially when SLA conditions are not fulfilled (e.g. elasticity, data localization).
8. Seamless change of provider (CH8): enable to seamlessly change the service provider including all services, dependencies and associated data to avoid vendor lock-in and to be able to quickly react in situations which may cause outage of the service.

To overcome these challenges we propose a framework to support a distributed Cloud Service environment of interoperable, legally compliant, self-monitored and reliable cloud services, through the ACSmI: Advanced Cloud Service Meta-Intermediator. Despite the high relevance of the problem, to our best knowledge it has not been formally proposed and validated in the literature a comparable Cloud Brokerage solution, addressing both the needs of the Cloud Services Providers and the requirements of the Cloud Services consumers and supporting the whole lifecycle of Cloud Services, from endorsement and discovery to monitoring and operation.

2.2 Analysis of related work and state of the technology

Following the work done in (Ibarra et al., 2016), (Alonso et al., 2017b), and (Juncal Alonso et al., 2019) the analysis of the most relevant existing Cloud Broker Solutions with respect to the identified challenges in section 1.1 is presented.
To carry out this study the challenges have been traduced into Key Functionalities (KF) for the anlysed existing solutions to fulfill (Table 1):

Table 1. Relationship between ACSmI key functionalities and detected challenges for Cloud Services Brokerage.

Key feature	Related challenge
KF1-Mechanisms to authorize and manage different roles and profiles	CH1, CH6
KF2-Services endorsement with complete information	CH5, CH6
KF3-Information about the status services for the CSPs shall be available	CH7
KF4-Intelligent discovery (including ranking) of services based on NFRs selected	CH4, CH5
KF5-Contracting and billing functionalities for different providers	CH1
KF6-Deployment mechanisms	CH4, CH8
KF7-NFRs monitoring	CH2, CH3, CH4, CH6

Trying to cover existing solutions with different maturity in terms of technology readiness the analysis has included Cloud providers such as Amazon WS, HP and IBM, as well as other big players such as Cisco or Oracle. At the same time, both commercial solution providers (such as Appcara AppStack and Jamcracker Service Delivery Network) and Open Source initiatives (Ubuntu Juju) which are developing solutions that enable the creation of customized cloud marketplaces have been studied.Targeting specifically the European research community, Helix Nebula Marketplace , established by a combination of public and private organizations specifically addressing European legal and regulatory requirements has been identified also as relevant for the study.
In another segment, Governmental Cloud marketplaces continue to growth in number and influence. Gov.apps in the US was the first one to appear, but soon others summed up to this trend: UK with Digital Marketplace (previously CloudStore offered under G-Cloud) and other on-going initiatives in Australia and New Zealand. Both US (Gov.apps) and UK (Digital Marketplace) Cloud marketplaces are operated from Government institutions: GSA (US General Services Administration) and UK Government Procurement Service as part of the G-Cloud Programme. For instance, US GSA offers consolidated contracting to negotiate better prices and reduce administrative costs for US Government agencies purchasing goods and services through GSA schedules. At European level, efforts are finally being invested in a European Federated Cloud through the Gaia-X project (DE-CIX Management GmbH et al., 2020), in collaboration with German and French governments, which first proof of concept for the design of the European cloud are set to be ready towards the end of 2020[1].
Different solutions have been evaluated, from the more stable ones (already commercialized in the market) to the most innovative ones (provided as research project results). More concrete, 8 commercial solutions, 3 open source products, 3 public administration solutions and 9 solutions coming from research projects have been analyzed.
In figure 2 their coverage with respect to the key features described in table 1 is presented.
From this analysis the following conclusions can be extracted:

- The mechanisms for the governance of the services are covered by almost all the analyzed solutions.
- The features related with the intelligent discovery and the assessment of the SLA are not covered in the majority of the solutions.

[1] Gaia-X has not been included in the study as in the moment where this paper was written the first prototypes were not implemented.

- Most of the commercial solutions do not cover or only cover partially the majority of the key features identified. Indeed a few of them cover the functionalities related to automatic multi-cloud deployment and NFRs monitoring.
- EU funded projects address the majority of the challenges identified (except the intelligent discovery) but they do not offer a complete solution as they are not focused on multi cloud applications and their needs.
- None of the existing solutions cover all the identified challenges/features that are relevant for multi-cloud scenarios.
- The proposed solution ACSmI can contribute to relevant modules of the European Gaia-X initiative for the federated catalogue of services, continuous monitoring, certification and accreditation of CSs.

3 Solution proposal

3.1 ACSmI: Detailed technical design of an Advanced Cloud Service meta-intermediator

The Advanced Cloud Service (meta-) intermediator (ACSmI) (Escalante, 2019) aims to provide the means for the discovery, contracting, managing and monitoring of different cloud service offerings. ACSmI also provides means to continuously assess the fulfilment of non-functional properties of cloud service offerings while enforcing the legislation compliance.
ACSmI can be described and understood considering the different phases that a Cloud Service will go through during its lifecycle (see Figure 3). In this respect, while some standardizations efforts are centered on the application lifecycle (i.e. TOSCA (OASIS, 2013)) or in the Cloud SLA lifecycle (Trapero and Suri, 2016)) up to our knowledge no work has been published centred on the Cloud Service lifecycle. In the case of the intermediation of Cloud Services it is relevant to be aware of the different phases that a Cloud Service passes through from the point of view of the Cloud Service Broker. These phases have been defined considering the different actors that has a role in the ACSmI. They are based on the roles defined by NIST in the Cloud Computing Standards Roadmap (NIST Cloud Computing Standards Roadmap Working Group, 2013):

- Service initialization, including cloud service endorsement into the broker, (Federated) intelligent discovery of services, (Federated) service contracting, CSLA provision, Users management in the broker, Security Management and Creation of the aggregated services in the Service Broker.
- Service operation, including CSLA monitoring, legislation compliance, data migration/portability, service metering, Billing to the user, and CP costs estimation.
- Service termination: including service withdrawal and service contract termination:

ACSmI has been designed to support these activities (Figure 4). Four main conceptual components are in charge of the implementation of the core functions:

- Service Management oversees the execution and management of all the operations related to the services offered by ACSmI. Functions like Cloud Services endorsement, intelligent discovery, or service operation are covered.
- Cloud Service SLA monitoring implements the monitoring functionalities: 1) Collects the different SLA terms that will be monitored and selects the metric/parameters associated to each term, 2) stores the collected data, 3) continuously assesses the compliance of the SLA of the contracted services and informs the user if an anomaly occurs and 4) notifies the CSLA violation to the CSP.
- Legislation Compliance is responsible of the assessment of the information collected from the CSPs with respect to the requirements set by the applicable legislation, as requested by the user when defining the NFR. This module is also in charge of the assurance of the propagation of the changes in the legislation through all the services inside the service registry with the corresponding assessment and also it is responsible of showing how contracts are terminated as well as what terms regulate the termination of a service, e.g. data format on exit, data portability, security measures etc.

- Business Model management which executes and manages of all the operations related to Service Contracts in ACSmI. It also performs all the activities related to the financial operations with the different users.

These conceptual modules have been technically traduced in the following software components, from section 3.1.1 to section 3.1.5.

3.1.1 ACSmI Discovery

ACSmI Discovery component (service management in Figure 4), covers the discovery and endorse functionalities, as well as the modification and deletion of the services endorsed in the service registry. The discovery and endorsement of the services is performed based on common attributes for each service type class. Figure 6 shows the class model of the ACSmI discovery component.

For the final prototype, three service classes have been defined with the corresponding service attributes, namely "Storage", "Database", and "Virtual machine". It is to be said that the approach followed allows the easy enlargement of the service classes to new type of services (i.e. edge nodes services in the case of IoT based systems). The rationale behind this design for the service catalogue is based on the assumption that the ACSmI will integrate both general purpose Cloud vendors such as Amazon as well as small niche oriented ones (i.e. Aimes https://www.aimes.uk/ who is specialized on Cloud solutions for the Health sector).Table 2 shows the relationship between the service type and the attributes of each service. Similarly, the selection of the current attributes is used to describe the services including relevant characteristics that a DevOps team will need when seeking for Cloud Services (Figure 7). The selection of the current ones was based on the requirements elicited from the use-cases used for the initial validation of the solution (section 4). Like the service classes, attributes can be extended to include new services properties. Any CSP that wants to endorse their cloud services in the service registry is required to provide this information (Figure 7).

Table 2. Attributes for each cloud service class in the ACSmI Discovery

Storage	**DataBase**	**Virtual Machine**
Region	Region	Region
Zone	Zone	Zone
Provider	Provider	Provider
Storage type	Database type	Virtual CPU cores
Storage subtype	Database technology	Frequency per core
Storage capacity	Data transfer IN	Memory
Storage data redundancy	Data transfer OUT	Instance storage
Availability	Virtual CPU cores	Optimized for
Request – Response time: Storage Performance	Database storage capacity	Public IP
Legal certifications/ accreditations	Availability	Underpinning technology
Cost/Currency	Transaction Unit (DTU): Database performance	Availability
	Legal certifications/ accreditations	Response time: Virtual Machine Performance
	Cost/Currency	Legal Level/accreditations
		Cost/Currency

3.1.2 ACSmI business model management

ACSmI Business model Management component (Business Model Management Figure 8), is responsible for the execution and management of the core functions with respect to the contracting and billing of the Cloud Service:

- Contracting: The prototype allows to establish contracts with Cloud providers to use their resources through the ACSmI. For this Cloud providers need to offer APIs, so that ACSmI contract the services programmatically.
- Manage CSPs: To deploy the software onto an infrastructure user needs to have an access. The prototype offers the possibility to the user to provide their own credentials for a concrete Cloud provider or to establish a new contract. Once established, the existing contract can be reused.
- Billing: It also includes features for setting specific rules for contract(s) billing, tracking the usage information, charging users in accordance with the defined rules and providing billing and usage-related reports both to the provider and to the monitoring component.

The current prototype of the ACSmI Contracting component is an extension of the Cloud Broker platform (http://cloudbroker.com/). It supports the situations when contracting is requested for more than one resource. For this prototype, pre-defined contracts have been stablished with Amazon and Microsoft Azure. The case when the automatic contracting is not supported by the Cloud Service provider is also offered by ACSmI contracting. This is the case of most of the small, sector specific Cloud Services providers. Different possible contracting workflows are shown in Figure 9.

3.1.3 ACSmI monitoring

ACSmI Monitoring component (SLA Monitoring in Figure 10) monitors the fulfilment of the SLAs for each Cloud Service contracted. QoS monitoring and SLA verification is an important source to verify trust and to adjust trust. If the monitoring is conducted by a Cloud Broker, then the belief in the results of monitoring is dependent on the trust in that broker with respect to objective and professional monitoring (Huang and Nicol, 2013). Existing tools such as Nagios or Ganglia provides means to monitor low level metrics of computing resources in general, but still automation on the configuration and calculation of complex metrics to assess CSLAs is still missing, especially when addressing multi-cloud environments. Some attempts (Ward and Barker, 2015) have been performed to address the elasticity and scalability inherent to Cloud deployments but with no focus on the monitoring of specific metrics to properly assess actual CSLAs contractually relevant. ACSmI monitoring assess the SLAs (referred as non-functional properties) of the services offered by the CSPs to detect any violation of the SLAs. If a violation is detected, an alert to the CSP will be sent. In ACSmI, the NFRs to be assessed are performance, availability, location and cost. These have been selected considering the needs and preferences of the Use Cases used for the validation of the solution (section 4). Nevertheless, as with the other modules the design has been made to be extendable with new non-functional requirements. For the current implementation only virtual machines (IaaS) have been considered.

For each of the selected Non-Functional Requirement, related metrics to be assessed have been defined. With the objective of being able to compare and combine the SLA from different CSPs the metrics are defined and expressed by ACSmI and compared to the SLOs provided by the providers. ACSmI supports ISO/IEC 19086-1:2016 standard (ISO, 2016) for the SLOs and the metrics definition. This standard seeks to establish a set of common cloud SLA building blocks (concepts, terms, definitions and contexts) that can be used to create Cloud Service Level Agreements (CSLAs). In ACSmI prototype the authors have used the MCSLA core library (Dutkowski, 2019) which up to our knowledge is the only implementation of the standard. The instantiation of such library for the usage of ACSmI monitoring has implied the definition of the corresponding parameters such as metric, Expression, Parameter, Remedy, ViolationTriggerRule, UnderlyingMetricRef, which are terms required by the standard. SLAs from the cloud service providers should be as descriptive as possible, and they should especially contain metrics that allows the customer to monitor the fulfillment. On the contrary, this is rarely the case.

The definition of a compound SLA for a Multi-Cloud application is another issue that needs to be tackled by ACSmI. The former library supports the definition of different aggregation patterns for composed Service Level Objectives. This is crucial when addressing Multi-Cloud applications, for which the composed Multi-Cloud SLA (MCSLA) (Dutkowski, 2019) is based on the composition of the underlying Cloud services SLAs' on which the different components are deployed. The MCSLA can act as the contract between the end-users and the developer of the multi-cloud native application and it needs to be assessed at run time. The fulfillment of such MCSLA depends on the individual Cloud Services and their own CSLAs.
An MCSLA must therefore act as an aggregator of all terms defined in the various SLAs, as shown in the next formula with Availability:

$$MultiCloudAvailability\ (term_1,\ldots,term_n) = 100\% - (\sum (100\% - term_i))$$

A graphical representation of this approach supported by ACSmI monitoring is shown in figure 11.
The solution proposed in ACSmI combines push monitoring (internal approach for monitoring VMs) and pull monitoring (external approach for monitoring VMs) (Alcaraz Calero and Gutiérrez Aguado, 2015) for cloud resources. Initially push monitoring was selected as the candidate path to be followed due to its independency and low intrusion levels. After some testing it has been decided to follow a combined approach to be able to address some of the proposed metrics such as performance at resource level that with the push monitoring approach was impossible to get. Technically this implies the incorporation of pre-configured agents to be installed in the corresponding virtual machines, in what is called Extended Internal Adaptive Architecture (Alcaraz Calero and Gutiérrez Aguado, 2015). As the definition of the NFRs differ from one CSPs to others and being far of having a common approach, the set of metrics to assess the selected NFRs have been specifically defined for ACSmI. This strategy allows to compare, compose and assess the values in a consistent way for different Cloud providers. On the contrary, it enforces the Cloud providers to provide specific metrics for the SLOs defined by ACSmI. In this case and in order to support the most standardized metrics, the guidelines defined in ISO/IEC 19086-1 and in the literature (Ataie et al., 2017) and practitioners (i.e. Cloud Service providers) have been adopted. The metrics related to these definitions are the ones which are monitored and compared:

- Availability. This NFR has defined as:
  $Availability = MTBF/(MTBF+MTTR)$
  This composed metrics are calculated based on other discrete metrics using different techniques (i.e. responses to the ping command).
- Performance. For the performance the usage of CPU, memory and disk is measured. For the current prototype, ACSmI monitoring is initialized to the 80% of the values in each category (i.e. 80% disk usage) but different thresholds can be established and configured ad hoc through the ACSmI monitoring API.
- Location. This NFR determines where a cloud resource is located, geo-locating its IP address from the Service registry. The information that relates the IP addresses with their real time locations is taken from MaxMind GeoIP2 Java API with the free GeoLite2 database.
- Cost. This NFR determines the current cost that a CSP is reporting on a certain resource. The actual incurred cost per Cloud Service is monitored through the ACSmI billing API (described in section 3.1.2) which provides information on the usage and the incurred costs in a certain period of time (configurable).

During the monitoring process, if any of the stablished SLAs is violated the ACSmI monitoring component generates an alert for the operator of the application (through an email) and updates the ACSmI discovery Service Registry information to support the future selection or discard of a Cloud Service.
Figure 12 and figure 13 show examples of the implemented ACSmI monitoring component GUI.

3.1.4 ACSmI legal

ACSmI legal (Legislation Compliance in figure 14) aids in the support of the assurance of the legal compliance of a Cloud service to be endorsed into the ACSmI registry.

In order to enable such a functionality, a legal expert as part of the entity exploiting ACSmI will be in charge of performing a legal compliance analysis of the services. ACSmI legal component, supports the legal expert by easing the collection of legal related documents and information and characterizing the services under a legal level taxonomy. The classification of the Cloud Service under this taxonomy will provide the users of those services with relevant information about the regulations and legally relevant certifications supported. For this, each Cloud Service is assigned with a legal level (tier 1, 2 or 3, tier 1 being the highest), based on an extensive questionnaire and guidelines set supporting the legal interpretation of the existing legal compliance situation of a certain Cloud Service.

The assessment of the legal compliance is based on information to be provided by the CSP, namely:

- The service contract applicable to the service
- The SLA applicable to the service
- The Data processing agreement governing the service
- Any other contract also governing the service, if any

In (Gryffroy, 2019) all the legal controls used in ACSmI are extensively explained. For the determination of the legal level, only legal controls which information can be assessed "*in concreto*" are considered. Firstly, based on the contractual documents provided by the CSPs when onboarding their service into ACSmI, and secondly, based on other pieces of information that CSPs might be required to provide in addition to those contracts, i.e. by answering a limited list of questions to obtain legal information which is relevant but not (typically) provided in a contract (e.g. the presence of a DPO at the CSP).

These contracts are uploaded to the ACSmI registry when the CSP endorses its services. Moreover, when endorsing its services, the CSP must answer a questionnaire and based on these answers and on the analysis of the CSPs contracts the existence of two types of controls are stablished:

- 8 controls related to the 8 yes/no questions asked to the CSP. They are called "simple controls" and can either be present (✓) or not present (×).
- 26 controls related to an assessment of the contracts offered by the CSP by the legal expert. They are called "layered controls". These controls relate to legal topics and ensure a minimum level of legal protection and/or safeguards is/are present. If any of these layered controls are present, no legal level will be assigned, and the service cannot be endorsed into ACSmI. Based on the number/characteristics of the layered controls found the service is classified in one of the following categories: basic legal safeguards present (★), substantial legal safeguards (★★) or strong legal safeguards (★★★).

This leads to a matrix where the relationship of the controls and the legal level is related. In table 1 an excerpt of this matrix is shown:

Table 3. Excerpt of the controls and the related ACSmI legal level.

Control	Legal level tier 3 (basic legal safeguards)	Legal level tier 2 (substantial legal safeguards)	Legal level tier 1 (strong legal safeguards)
		Simple controls	
Valid company registration	✓	✓	✓
DPO contanct	✓	✓	✓
Representative	✓	✓	✓
Data transfer mechanisms	✓	✓	✓
Data Processing agreement	✓	✓	✓

ISO 27001 or equivalent	×	✓	✓
		Layered controls	
Assessment of Alternative Dispute Resolution mechanisms	★	★	★★
Termination options of CSPs counterparties	★	★	★★
Liability coverage	★	★	★★
Force majeure coverage	★	★	★★

Based on the answers and the analysis by the legal expert of the CSP contracts, a legal level will be assigned to the Cloud service being endorsed.

3.1.5 ACSmI: Technical implementation

The presented technical design was implemented in a modular way, providing several interfaces. In table 4 the technologies used for each of the modules are presented.

Table 4. ACSmI technologies per software component

ACSmI component	Baseline technologies	Implementation language
ACSmI discovery	JHipster	Java
ACSmI contracting	Cloud Broker Platform	Ruby on Rails
ACSmI monitoring	Telegraf, InfluxDB	Java
ACSmI billing	Cloud Broker Platform	Ruby on Rails
ACSmI legal	None	Java

The solution was implemented and deployed for experimentation in TECNALIA premises, in Derio (Spain). The code has been released as open source code and is available in a gitlab public repository[2].

4 Experiments and solution validation

Four testing cases have been implemented to validate ACSmI, three from the infustry (real experiments with software applications at production stage) and one from the research field. They are microservices based applications with specific Non-Functional Requirements that are deployed in a Multi-Cloud topology using the presented ASCmI for the discovery, contracting and run time monitoring of the cloud services:

- **Clinical Trial Governance Platform**: A tool for academic health science researches to develop and manage clinical trials. Sensitive Personal Patient Identifiable Information is stored within this tool, and the data belongs to people who live in different countries across the world. Adopting the Multi-Cloud approach to address the legal ramifications of hosting sensitive data comes with specific critical NFRs in terms of security and legal compliance which is the main motivation for the selection of this testing case. For the validation exercise an architecture of 5 microservices has been used.
- **Blockchain-based energy trading platform**. This platform brings together energy producers and consumers, allowing the former to make energy offers and the latter to purchase power under the terms of the offer. The energy exchanges are

[2] https://git.code.tecnalia.com/DECIDE_Public/DECIDE_Components/-/tree/master/ACSmI

handled by means of smart contracts. For the ACSmI validation an instance of 3 microservices of the original system has been utilized.

- **Cloud Service provider incidence tracking**. An internal application to coordinate and monitor activities performed in the data centres of the Cloud Service provider (ARSYS https://www.arsys.es/. For the validation exercise the architecture tested was formed of 3 microservices.
- **Multi-cloud micro-services-based application (Sock Shop)**: The Sock Shop App[3], is a loosely coupled microservices demo application. It simulates the user-facing part of an e-commerce website that sells socks. The Sock Shop app is designed to provide as many microservices as possible. In the case of ACSmI validation the Sock Shop has served as an additional "use case" application to guarantee the scalability of the solution as it includes 9 microservices while the other use cases include 2 or 3. In this experiment the Sockshop application has been deployed into 1 Cloud Service provider (but different Cloud Cervices of such provider) and two different Cloud Services providers over multiple services.

The proposed solution has been evaluated under different perspectives, User centred testing to test the fulfilment of the use cases needs), requirements achievement tracking to assess the functionalities offered with respect to the functional requirements elicited) and Business centred evaluation to indicate the benefits that it brings to the companies that make use of it.

In this article only the results from the Business Centred Evaluation are reported and discussed.

For that, an estimation of the effort needed to manually perform the activities corresponding to different processes under the Cloud Service Lifecycle have been reported by the Use Case owners, Cloud Services Intelligent Discovery, Cloud Services Contracting and Cloud Services Monitoring. Then the effort needed for the same activity has been calculated using ACSmI. This is then translated to costs based on the characteristic of each company and project.

An example of the process followed for the Business centered evaluation for the Intelligent Discovery process is included in table 5.

Table 5. Resources needed to perform the activities included in the Intelligent Service Discovery process, under the Cloud Service Lifecycle.

Cloud Service Intelligent Discovery process	Broken down activities	Effort needed PH: Person/hour PM: Person/month	Effort needed with ACSmI	Saved effort
	Study the existing available Cloud Services from different providers	2PH	0.5PH	2PH
	Analyse the characteristics of each Cloud Service (SLAs, costs, supported technologies, third party components dependencies, etc.)	8PH	0PH	8PH
	Be aware of run-time information of specific Cloud Services with respect to SLA violations so that these Cloud Services can be discarded when selecting the most appropriate ones.	0,5 PM	0PH	60PH

In figure 15 the effort needed to perform all the activities from each of the processes is reported. The effort is reported in person/hour for the main three processes, Cloud Service Discovery, Cloud Service Contracting and Cloud Service Monitoring in terms of the estimation of the needed effort to implement the activities o complete the corresponding phase. For this validation exercise in figure 15, graphic a) the same application is deployed in the same number of Cloud providers both manually and using ACSmI. In figure graphic b) the same application is deployed firstly into one service provider and secondly into two services providers. This exercise allowed us to compare on the one hand the advantages brought by ACSmI when the complexity

[3] https://microservices-demo.github.io/

of the application increases (in terms of microservices number) and on the other hand the benefit provided by ACSmI when, with the same application complexity (the same number of microservices) the number of Cloud providers increases.
The unit to measure the effort is the person hour. In this way the results from the different companies can be compared independent from their internal structural cost based on their size or industrial sector.
In figure 15 a) the colour code is as follows:

- Blue results correspond to the Cloud Service provider Incidence Tracking application deployed in one Cloud provider (Arsys). Dark blue for the effort needed to perform each task manually and light blue depicts the effort needed to perform each task using ACSmI.
- Yellow results correspond to the Clinical Trial Governance Platform deployed in two Cloud providers (Aimes and Amazon). Light yellow for the effort needed to perform each task manually and dark yellow depicts the effort needed to perform each task using ACSmI.

Therefore, in figure 15 a) two applications are compared, one with two microservices deployed in a single Cloud provider and another one with 4 microservices deployed in two different Cloud Service providers. In both cases the developer saved effort when they used ACSmI in the Cloud Service Contracting and monitoring processes. The developers reported that the effort saved in the monitoring process (up to the 80 %) is mainly due to the proactive continuous monitoring which allowed the developers to assure the fulfilment of the CSLA contracted in terms of accomplishment of the selected non-functional requirements (availability, location and performance). When the number of Cloud providers increases the savings are extended to the discovery phase. The developers reported that analysing the needs of each microservice and each Cloud Service provider is a time-consuming task, even more when the offer is disaggregated and described in different terms.
In figure 15 b) the color code is as follows:

- Blue results correspond to the Sockshop deployed in one Cloud provider (Amazon). Dark blue for the effort needed to perform each task manually and light blue depicts the effort needed to perform each task using ACSmI.
- Yellow results correspond to the Sockshop deployed in two Cloud providers (Amazon and Azure). Light yellow for the effort needed to perform each task manually and dark yellow depicts the effort needed to perform each task using ACSmI.

In this case the savings achieved when using ACSmI are greater. In the three phases the effort saved is relevant, more than the 90%. Now, as 9 microservices are composing the application, the analysis of which Cloud Service fits better (Intelligent Service Discovery) requires much more effort than in the previous case. Subsequently the benefits reported when using ACSmI for this purpose are also greater.
From this, it can be deduced that when the number of CSPs grows the benefits of using ACSmI increases exponentially.
In figure 16 the different effort saving percentages are shown for the different experiments. The savings produced by ACSmI increases both with the application complexity (in terms of microservices number) and the number of Cloud Services to be used in each case. Of course, some deviations may exist as the exercises have been made by different DevOps teams.

5 Conclusions and future work

This paper describes ACSmI, a Cloud service meta-intermediator for automatic Cloud Service discovery, contracting, proactive monitoring and CSLA assessment. ACSmI was designed to hide the complexity of Cloud infrastructure selection and management and to support dynamically the monitoring of the services to ensure the fulfilment of the SLOs with respect to certain non-functional properties such as location, performance, availability and cost, as part of the SLA. ACSmI is an extensible framework where common but crucial NFRs for the Cloud can be included both for services discovery and monitoring (i.e. load balancing, scalability, legal awareness). It has been proven, by a set of four experiments that the usage of ACSmI positively impacts the effort needed to discover, contract and manage multiple Cloud Services at run-time.

ACsmI also contributes to relevant elements of the European Gaia-X initiative, specifically to the federated catalogue, continuous monitoring, and certification of services.

As part of the future work, it is planned to further investigate new requirements in an edge-cloud environment, including the characterization of edge nodes and network services as available resources to be selected and brokered through the framework. This will require the extension of the taxonomy for the service registry as well as the adaptation of the monitoring mechanisms and techniques. Moreover, it is expected to extend the work on the legal aspects to be incorporated into the monitoring phase so that the legal level is included in the continuous monitoring phase. To this respect the approach can be broaden to the incorporation of compositional certification monitoring feature, assuring that the composition of monitoring metrics from the Cloud Services fulfils the evidences required by the certification scheme at any time. In this case new monitoring parameters, metrics and the related techniques to acquire and securely store them shall be put in place.

6 References

Alcaraz Calero, J.M., Gutiérrez Aguado, J., 2015. Comparative analysis of architectures for monitoring cloud computing infrastructures. Future Generation Computer Systems 47, 16–30. https://doi.org/10.1016/j.future.2014.12.008

Alonso, J., Orue-Echevarria Arrieta, L., Escalante, M., Benguria, G., Echevarria, G., 2017a. Federated Cloud Service Broker (FCSB): An Advanced Cloud Service Intermediator for Public Administrations, in: Cloud Computing and Service Science. Presented at the 7th International Conference on Cloud Computing and Services Science, Springer, Porto, p. 391. https://doi.org/10.5220/0006285003840391

Alonso, J., Orue-Echevarria, L., Escalante, M., Benguria, G., 2017b. DECIDE: DevOps for Trusted, Portable and Interoperable Multi-Cloud Applications towards the Digital Single Market, in: Proceedings of the 7th International Conference on Cloud Computing and Services Science, CLOSER 2017. Presented at the International Conference on Cloud Computing and Services Science, SCITEPRESS - Science and Technology Publications, Lda, Setubal, PRT, pp. 397–404. https://doi.org/10.5220/0006292403970404

Alonso, J., Stefanidis, K., Orue-Echevarria Arrieta, L., Blasi, L., Walker, M., Escalante, M., López, M., Dutkowski, S., 2019a. DECIDE: An Extended DevOps Framework for Multi-cloud Applications. https://doi.org/10.1145/3358505.3358522

Alonso, J., Stefanidis, K., Orue-Echevarria, L., Blasi, L., Walker, M., Escalante, M., López, M.J., Dutkowski, S., 2019b. DECIDE: An Extended DevOps Framework for Multi-cloud Applications, in: Proceedings of the 2019 3rd International Conference on Cloud and Big Data Computing, ICCBDC 2019. Association for Computing Machinery, New York, NY, USA, pp. 43–48. https://doi.org/10.1145/3358505.3358522

Ataie, E., Entezari-Maleki, R., Rashidi, L., Trivedi, K., Movaghar, A., 2017. Hierarchical Stochastic Models for Performance, Availability, and Power Consumption Analysis of IaaS Clouds. IEEE Transactions on Cloud Computing PP, 1–1. https://doi.org/10.1109/TCC.2017.2760836

Balouek-Thomert, D., Renart, E.G., Zamani, A.R., Simonet, A., Parashar, M., 2019. Towards a computing continuum: Enabling edge-to-cloud integration for data-driven workflows. The International Journal of High Performance Computing Applications 33, 1159–1174. https://doi.org/10.1177/1094342019877383

DE-CIX Management GmbH, Eggers, G., Fondermann, B., Google Germany, Maier, B., Ottradovetz, K., Pfrommer, J., Reinhardt, R., Hannes, R., Schmieg, A., Steinbuß, S., Trinius, P., Weiss, A., Weiss, C., Wilfling, Sabine, 2020. GAIA-X: Technical Architecture. Federal Ministry for Economic Affairs and Energy (BMWi).

Dutkowski, S., 2019. D3.15 Final multi-cloud native application composite CSLA definition.

Elhabbash, A., Samreen, F., Hadley, J., Elkhatib, Y., 2019. Cloud Brokerage: A Systematic Survey. ACM Comput. Surv. 51, 1–28. https://doi.org/10.1145/3274657

Escalante, M., 2019. D5.4 Final Advanced Cloud Service meta-Intermediator.

ETSI, 2013. Cloud Standards Coordination.

European Commission, 2020. A European strategy for data.

Fortiş, T.F., Munteanu, V.I., Negru, V., 2015. A taxonomic view of cloud computing services. IJCSE 11, 17. https://doi.org/10.1504/IJCSE.2015.071360

Gryffroy, P., 2019. D5.4 Final Advanced Cloud Service meta-intermediator (Annex).

Huang, J., Nicol, D.M., 2013. Trust mechanisms for cloud computing. J Cloud Comp 2, 9. https://doi.org/10.1186/2192-113X-2-9

Ibarra, J.A., Orue-Echevarria, L., Escalante, M., Benguria, G., 2016. Empowering Services based Software in the Digital Single Market to Foster an Ecosystem of Trusted, Interoperable and Legally Compliant Cloud-Services:, in: Proceedings of the 6th International Conference on Cloud Computing and Services Science. Presented at the 6th International Conference on Cloud Computing and Services Science, SCITEPRESS - Science and and Technology Publications, Rome, Italy, pp. 283–288. https://doi.org/10.5220/0005893302830288

ISO, 2016. ISO/IEC 19086-1:2016(en), Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1: Overview and concepts.
Jambunathan, B., Y., K., 2016. Microservice Design for Container based Multi-cloud Deployment. International Journal of Engineering and Technology (IJET) 8.
Juncal Alonso, Leire Orue-Echevarria, Marisa Escalante, 2019. Contribution to the uptake of Cloud Computing solutions: Design of a cloud services intermediator to foster an ecosystem of trusted, interoperable and legal compliant cloud services. Application to multi-cloud aware software. https://doi.org/10.5281/zenodo.3748988
Jurg van, V., Flavia, P., 2011. Programming Amazon EC2. O'Reilly Media, Inc.
Mazzucca, J., Ed, A., 2015. Survey Analysis: Cloud Adoption Across Vertical Industries Exhibits More Similarities Than Differences (No. G00271486).
Michon, É., Gossa, J., Genaud, S., Unbekandt, L., Kherbache, V., 2017. Schlouder: A broker for IaaS clouds. Future Generation Computer Systems 69, 11–23. https://doi.org/10.1016/j.future.2016.09.010
Neelakanta, G., 2012. Broker-Mediated Multiple-Cloud Orchestration Mechanisms for Cloud Computing. National University of Singapore.
NIST Cloud Computing Standards Roadmap Working Group, 2013. NIST Cloud Computing Standards Roadmap (No. NIST SP 500-291r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.500-291r2
Nizamani, S.A., 2012. A Quality-aware Cloud Selection Service for Computational Modellers. University of Leeds.
OASIS, 2013. Topology and Orchestration Specification for Cloud Applications Version 1.0 (OASIS Standard No. Version 1.0).
Petcu, D., 2013. Multi-Cloud: expectations and current approaches, in: Proceedings of the 2013 International Workshop on Multi-Cloud Applications and Federated Clouds - MultiCloud '13. Presented at the the 2013 international workshop, ACM Press, Prague, Czech Republic, p. 1. https://doi.org/10.1145/2462326.2462328
Tordsson, J., Montero, R.S., Moreno-Vozmediano, R., Llorente, I.M., 2012. Cloud brokering mechanisms for optimized placement of virtual machines across multiple providers. Future Generation Computer Systems 28, 358–367. https://doi.org/10.1016/j.future.2011.07.003
Trapero, R., Suri, N., 2016. A Common Reference Model to describe, promote and support the uptake of SLAs.
Ward, J., Barker, A., 2015. Cloud cover: monitoring large-scale clouds with Varanus. Journal of Cloud Computing 4, 16. https://doi.org/10.1186/s13677-015-0041-9
Zhou, G.S., Du, W., Lin, H.C., Yan, X.W., 2019. An approach for public cloud trustworthiness assessment based on users' evaluation and performance indicators. IJCSE 19, 206. https://doi.org/10.1504/IJCSE.2019.100241

7 Figures

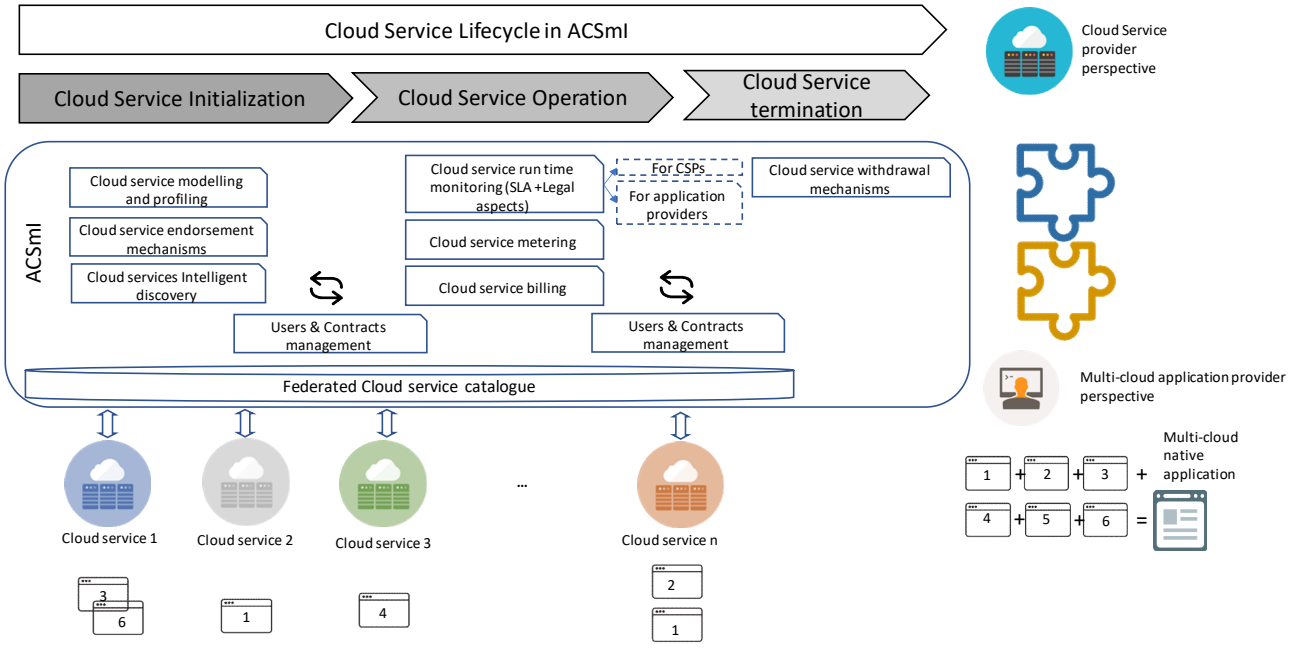

Fig. 1. Advance Cloud Service Intermediation, a solution for Cloud Service Federation towards the embracement of multi-cloud native applications by the European Software Industry.

Fig. 2. Coverage percentage with respect to the key functionalities of commercial solutions, research projects-based outcomes, open source frameworks and solutions from the public administration for Cloud Service Brokering

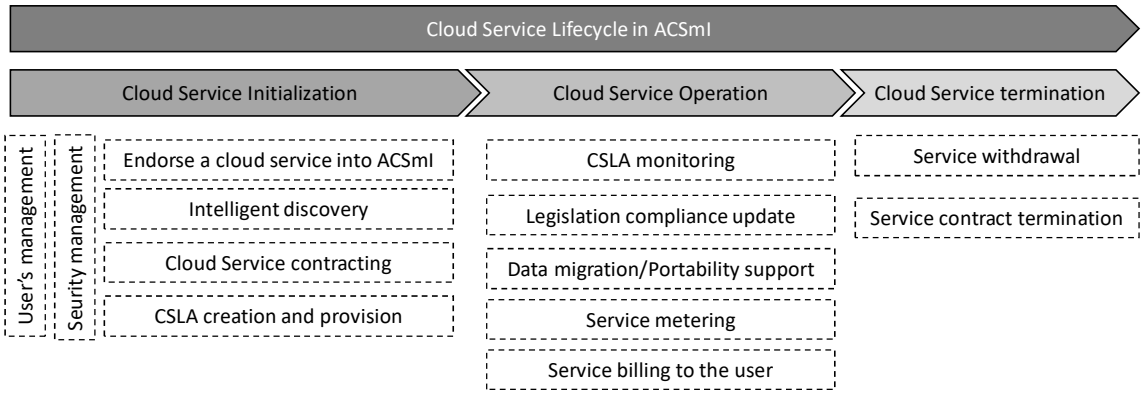

Fig. 3 The Cloud Service lifecycle in ACSmI

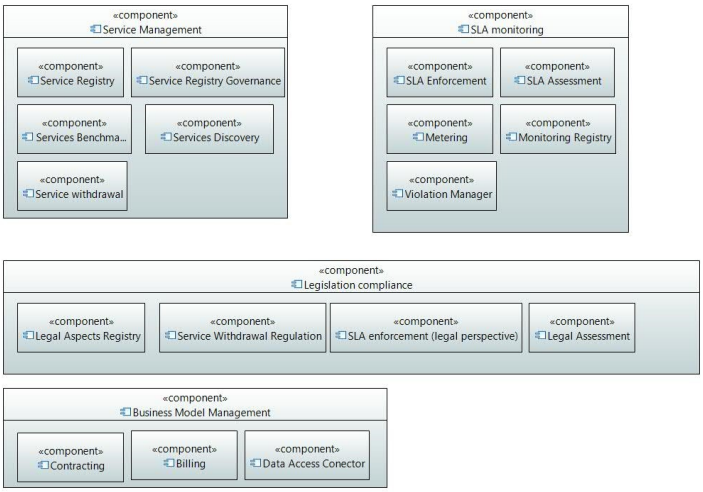

Fig. 4 ACSmI conceptual architecture

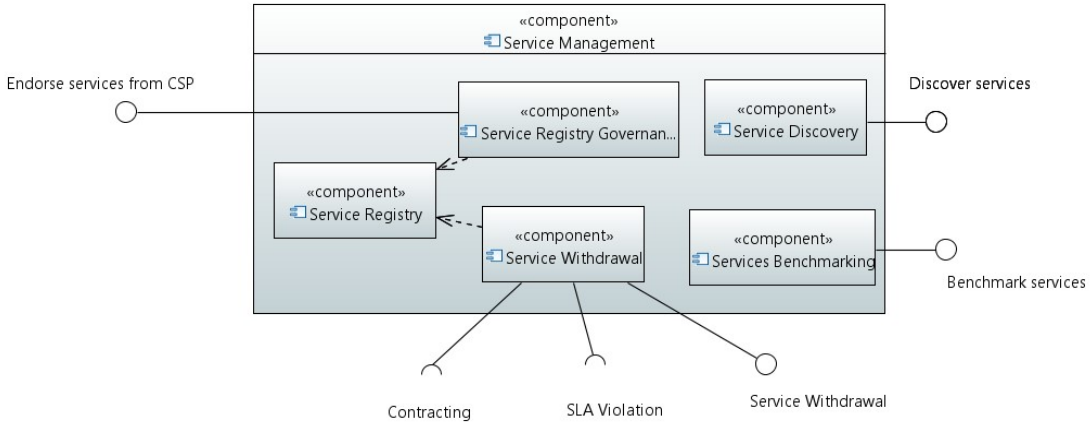

Fig. 5. ACSmI discovery high level component diagram

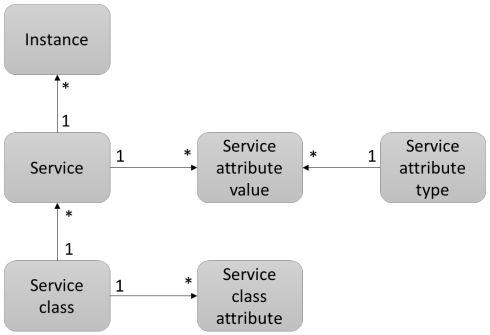

Fig. 6. ACSmI Discovery Service class model

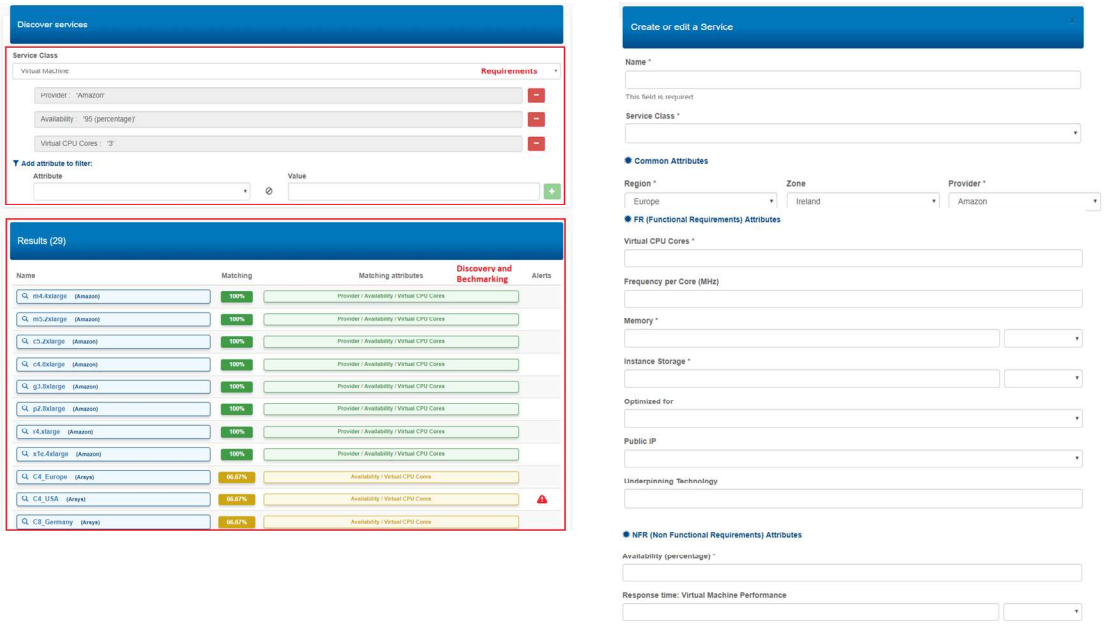

Fig. 7. ACSmI discovery UI for the Cloud providers (Cloud Service Endorsement) and Cloud Consumers (Cloud Service Discovery).

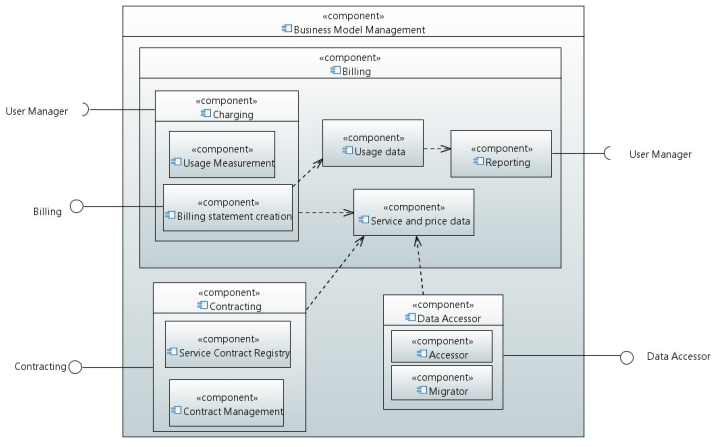

Fig. 8.ACSmI business model management component diagram

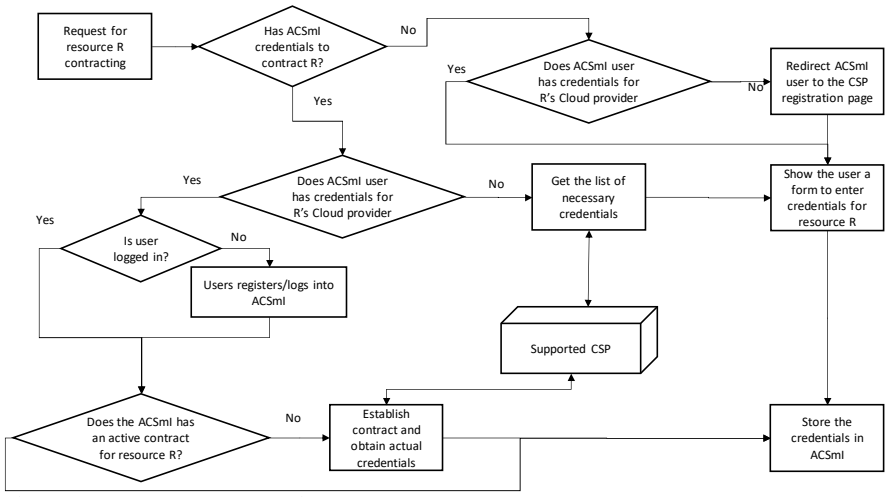

Fig. 9. Resource contract process in ACSmI

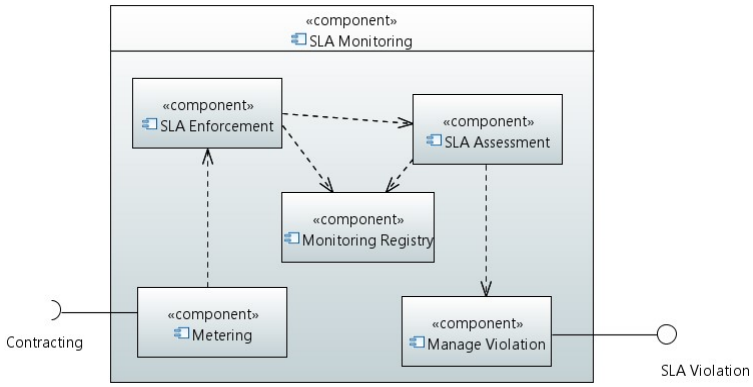

Fig. 10. ACSmI monitoring component diagram

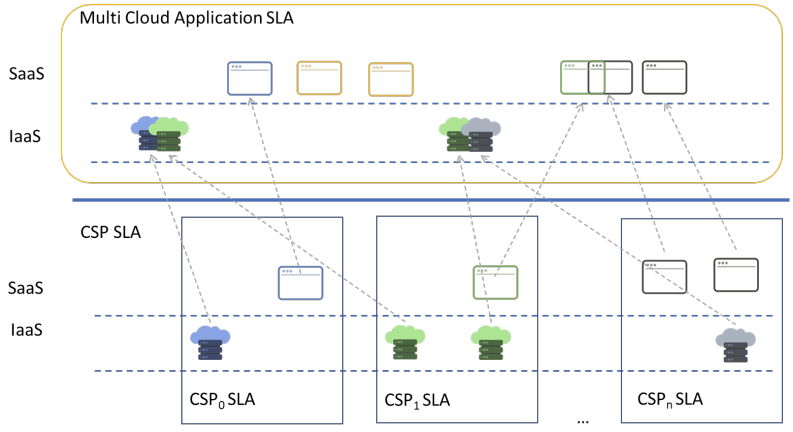

Fig. 11. Conceptual Idea – Make up of an MCSLA

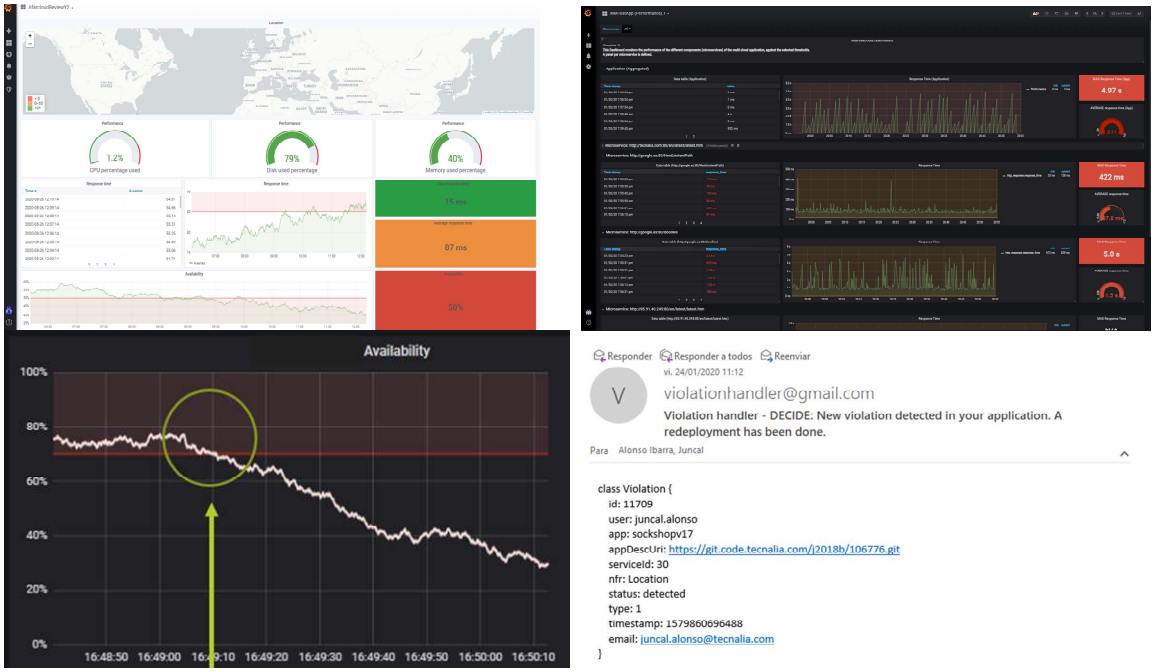

Fig. 12 ACSmI Cloud Resource Monitoring Grafana dashboards and detail of the email received after a location NFR violation

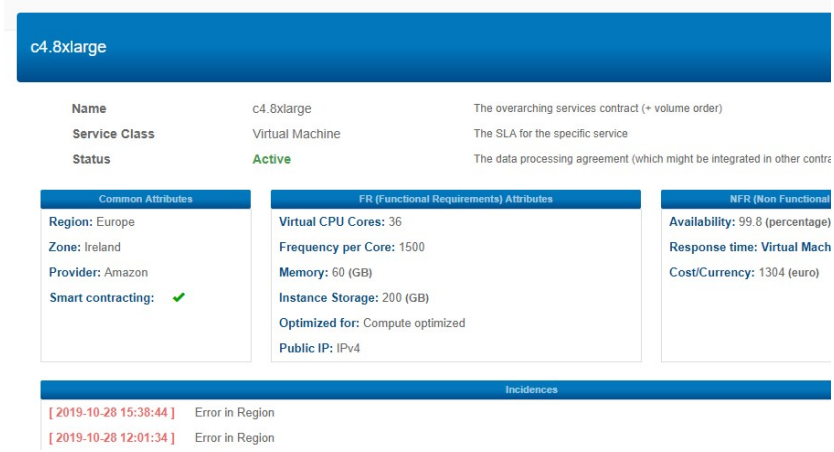

Fig.13 Detail of location violations registered in an ACSmI Cloud Service

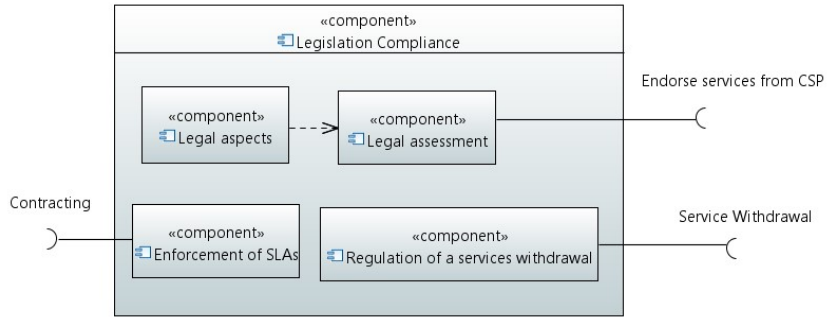

Fig. 14. ACSmI legal component diagram**.**

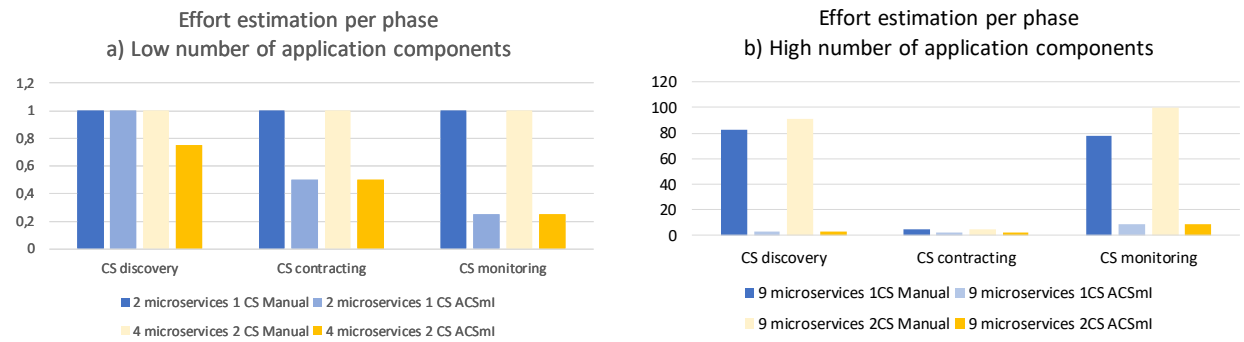

Fig. 15 Effort estimation per phase in the same and in different number of Cloud resources

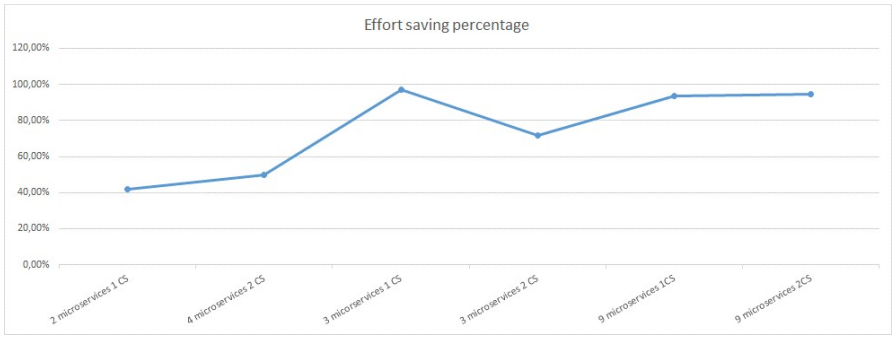

Fig. 16. Effort saving percentage