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

Juncal Alonso [1][a], Leire Orue-Echevarria[1][b] and Marisa Escalante[1][c]
[1] ICT Divsion, TECNALIA, Bizkaia technology park, Derio, Spain
{juncal.alonso, leire.orue-echevarria, marisa.escalante }@tecnalia.com

1 RESEARCH PROBLEM AND MOTIVATION

The digital transformation from product to service economy means changes in the companies' operating environment: they need to transform into service providers from product providers and be able to flexibly change their role in the value chain and markets. To be able to foster the change, the companies' IT infrastructure needs to be more flexible. Cloud services enable this to some degree, but as such create dependency to external partners for a company. In a world where new players come, others disappear, and conditions are continuously changing, how can the companies be sure that the architectural decisions that were taken in the past continue to be the best one? For example, while developing or migrating a web site, an organisation can decide to build it in a dedicated internal computer, build it as an instance in a shared internal computer, build it in a dedicated external computer, or even build it as an instance in a shared external. The decision on using one, another, or several approaches simultaneously is driven by certain evaluation criteria (e.g. profitability, reliability, performance, security, legal or even ecological aspects) and these criteria can be reviewed as new requirements arise driven by conditions change. Cloud providers themselves may fail too, so for the greatest measure of protection possible, an enterprise may wish to embark upon a multi-cloud strategy. There are several multi-cloud solutions available for solving specific problems, but to date, little attention has been paid to distributing the cloud risk and managing multiple clouds from a single technology platform. Working with many CSPs means managing multiple relationships. Most enterprises are already negotiating multiple contracts with multiple CSPs and multiple contracts mean multiple service level agreements, multiple payments, multiple passwords, multiple data streams, and multiple providers to check up on. That leads to questions about how to make those services work together, or how to unify all the efforts so maximum effectiveness and efficiency can be obtained. This is when a Cloud Service Broker (CSB) comes into play. A cloud services brokerage is a third-party software that adds value to cloud services on behalf of cloud service consumers. Their goal is to make the service more specific to a company, or 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. Consumers can leverage solutions offered by CSBs that allow organizations to focus on other pressing business needs instead.

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.

With so much activity implementing front-end and back-end applications in public, private and hybrid clouds, complexity has grown at every level (business, application, transaction and regulatory).

To generate meaningful results, it is envisioned that enterprises need to address key challenges (CH) in the next years (Alonso, et al., 2017):

1. Governance (CH1): Ensuring that services deployed in the cloud are protected is critical. Sharing can create leaks that cannot be tolerated. Fostering

[a] https://orcid.org/0000-0002-9244-2652
[b] https://orcid.org/0000-0002-0648-4689
[c] https://orcid.org/0000-0002-8624-6655

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): The resulting service intermediator shall support 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 cross-border 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. Moreover, a big challenge in this concern is to develop the methods and interfaces for securing legislation compliance and easy legislation change propagation through the cross-bordered and 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 localisation).

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 like bankruptcy of the cloud provider or any other cases which causes outage of the service.

A viable intermediator and federator of cloud services Broker (Alonso, et al., 2016) (Alonso, et al., 2017) 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 EU Member States.

2 OUTLINE OF OBJECTIVES

The main goal of this Thesis can be stated as follows:

Research the means, basic enablers, drivers, impact, risks and barriers and implement a solution for the re-use and combination of cloud services, for assembling a network of interoperable, legal compliant, quality assessed (against SLAs) single and composite cloud services for multi-cloud aware applications deployment and operation.

The main aim is to research, analyse, design, and develop an advanced cloud service intermediator (ACSmI) that supports the discovery, aggregation, and consumption of cloud service functionalities for multi-cloud applications. This goal can be broken down into the objectives:

I. Definition and implementation of the multi-cloud aware applications concept.

In this work we consider a multi-cloud native application as a distributed application over heterogeneous cloud resources whose components are deployed on different CSPs and still, they all work in an integrated way and transparently for the end-user. There are several reasons for deploying an application in a multi-cloud architecture, the most important ones being: non-compliance of the CSPs to the agreed SLAs, avoidance of vendor lock-in, increasing reliability or improving other QoS concerns such as increasing performance or security, and finally, reducing costs. The application types that would benefit the most from such a multi-cloud approach are on the one hand, those that are critical to the business and that need to respond efficiently to the user’s needs in terms of performance, reliability and security and on the other hand, complex applications whose components need to be distributed over different cloud providers due to their specific needs and requirements. Examples of these applications include: Network Management in extended multi-country scenarios with differentiated cloud layers, online videogames, Public Administrations online services, and travel agencies or ticket agencies (i.e. ticketmaster). However, any application offered as SaaS can benefit from a multi-cloud architecture. Currently, this is solved by deploying the same application on several cloud providers following a master-slave or active-passive approach. This, however, poses also several risks, since the synchronization of all the data is critical for a correct functioning of the application if no data loss is wanted. The multi-cloud approach to be included in this work tries to minimize synchronization risks and guarantee the fulfilment of the application providers' requirements, which can range from maintaining a constant cost structure to a certain response time, security issues or a certain performance level

II. Analyse and provide mechanisms to discover and select a combination of cloud services specific for multi-cloud aware applications.

The objective of this research is to provide means for the discovery, registration and management of cloud service providers and offerings into the Advanced Cloud Service metaIntermediator, so that these services can be published and accessible to be used. ACSmI will aggregate and intermediate not only resources provisioning services (Hardware as a Service-HaaS) but also Database as a Service (DBaaS), and Platform as a Service (PaaS). The goal is to provide advance methods for intelligent Cloud service discovery based on a set of specific requirements set up by the end-user.

III. Research and provide mechanisms to assess continuous real time verification of the cloud services non-functional properties fulfilment (Composite CSLA) including legal aspects.

Provision of mechanisms to assess continuous real time verification of the cloud services non-functional properties fulfilment including legal aspects. The intelligent protection within the presented approach will have the ability to provide compliance assessment capabilities that enable continuous monitoring of application during the application life cycle and provide policy deployment reassessment if required non-functional properties are not accomplished

The proposed solution will include means for monitoring and assessing that the aggregated and intermediated cloud offerings fulfill the corresponding SLA terms and conditions, including legislation and accreditation issues, security aspects and propagation of changes

IV. Study and develop means for seamless change of Cloud service provider enhancing the portability and interoperability of multi-cloud aware applications.

Lock-in has the potential to obstruct portability and interoperability, so it has been a significant source of frustration for organizations looking to take advantage of the many proven benefits of cloud computing. In 2012, a US Government Accountability Office report (US Government Accountability Office, 2012)seven major challenges to adopting the Office of Management and Budget's cloud-first policy for IT deployments. Of these, ensuring data portability and interoperability within the cloud is the most daunting due to the large number of competing cloud technologies for data storage and retrieval.

Currently, many cloud providers are offering service-based versions of traditional databases—such as Oracle and MSSQL and MYSQL, as well as popular NOSQL newcomers—alongside their proprietary services. Newer systems—such as Apache Cassandra, for instance—are maturing as data components and provide more portable and interoperable solutions.

Nonetheless, the data portability is still an issue when moving from one Cloud Service provider to another.

V. Research and analyse the advantages and disadvantages of different business models' options for federated Cloud Service Brokers.

A Cloud Broker solution can support different business models, depending on their customers focus, value proposition or monetization strategy.

These business-oriented decisions can impact at different levels in the design of the technical solution. The goal of this task is to develop methods and tools that enable the control, monitoring and billing of the use of the baseline services of the ACSmI. This task will enable the implementation of the "ACSmI for benefit" business model and related negotiated services, in order to support negotiated access and usage of the intermediator. Different business models for the ACSmI and for each of the ACSmI stakeholders will be explored. The required "ACSmI for benefit" modules will be modified accordingly so as to be able to exploit the finally decided business model(s).

3 STATE OF THE ART

3.1 Cloud Computing fundamentals and challenges

According to NIST (Mell & Grance, 2011) (Leire Orue-Echevarria Arrieta, 2011), Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The NIST definition of cloud computing defines three delivery models:

- Software as a Service (SaaS): The consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it is running. Examples: Salesforce.com, Gmail, Google Apps, GotoMeeting, Run My Process.
- Platform as a Service (PaaS): The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment (and possibly has some control over the hosting environment), but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework. Examples: Google App Engine, Microsoft Azure, Salesforce.com.
- Infrastructure as a Service (IaaS): The consumer uses "fundamental computing resources" such as processing power, storage, networking components or middleware. The consumer can control the operating system, storage, deployed applications and depending on the specific provider the consumer may control networking components such as firewalls and load balancers, even select the characteristics of the virtual image. Examples: Amazon EC2, Mozy, Nirvana.

Cloud computing refers to both hardware and systems software in the data centres that provide services and the applications delivered as services over the Internet. Those services have long been referred to as Software as a Service (SaaS). In fact, SaaS is a model of software deployment where an application is hosted as a service outside of the customer’s site and delivered to customers across the Internet.

A successful SaaS application, unlike any other traditional application, is built as a single instance but multitenant and shared among multiple customers on a common infrastructure (hardware and software). These architectural considerations added to other key functional, scalability, security and support requirements are not addressed in traditional software development, and thus need to be taken into account while adapting traditional applications architecture to SaaS.

There are four deployment models for Cloud services; these are private, community, public, and hybrid. A deployment model indicates the attributes associated with Cloud services specially the access attributes. (Mell & Grance, 2011)

- Private Cloud Services: The Cloud infrastructure is used and operated by the same organization. This is a highly trusted and secure model as in most cases the infrastructure is based locally within the organization. The disadvantages of this model include lack of elasticity; i.e. increasing or decreasing the size of the Cloud on-demand.
- Community Cloud Services: The Cloud infrastructure is shared and operated by a group of organizations, with all supporting policy, security and operations.
- Public Cloud Services: The Cloud infrastructure is available to the general public or business for use. This is owned by a large organization and is the most common form of Cloud deployment. Large organizations such as Amazon, Microsoft and Google offer this form of Cloud.
- Hybrid Cloud Services: The Cloud infrastructure is a combination of two or more types of Clouds. This model requires the sub models to be bound by standard set of communication rules. An example of this would be a community Cloud working with a public Cloud to handle untimely surge in resource demand.

There are several key challenges for both users and providers to enter and establish in this new distributed computing paradigm (Nizamani, 2012). Key challenges faced by the users in moving their data/services to Cloud platforms include the following:

- Choosing the right provider: With the variety of services offered by several CSPs, users may find it difficult to choose the right provider which matches their requirements. At present, there is no platform which provides information about the capabilities of all the CSPs.
- Security and Privacy issues: As several users may share the same physical infrastructure in a virtualized manner simultaneously, users are often concerned about the security and privacy of their data in the Cloud platform. This is an important issue because, the data/service storage/running location specific information is abstracted from the users in Cloud environments.
- Trustworthiness of CSPs: Users are concerned about the trustworthiness of the CSPs. This aspect is different from security because, trustworthiness conveys information pertaining

to the task execution such as adhering to Service-Level Agreements (SLA adherence) and reliability of task execution (such as handling node failure, meeting task deadline etc).

- Dealing with lock-in: In economics, vendor lock-in makes a customer dependent on a vendor for specific products and/or services making it difficult for users to choose another CSP without substantial switching costs. The switching cost includes possible end-of-contract penalties, charges for format conversion and data/application switching and possible additional charges for bandwidth usage.

From the provider's perspective, there are many challenges to be addressed for exploiting various features of Cloud platforms, including (Iyer & Ganesh, 2012):

- Understanding the market: New Cloud providers may need to understand the current market status in terms of the competitors in the domain, the user preferences in terms of the products/services they prefer most of the time, user preferences for various features such as security and trust requirements etc.
- 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 (Vliet & Paganelli, 2011). Dynamic pricing strategies are required to improve their performance and to attract more customers based on the market situation.
- Monitoring user profile: With competition among different providers, CSPs may be required to monitor the reliability of users in terms of the feedback given by them to decide user acceptance criteria. It also helps to avoid any unhealthy competition among the providers and users.

3.2 Federation of cloud resources and cloud application marketplaces

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 (Mazzuca, 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. A number of scenarios demonstrate these serial or simultaneous interactions among hybrid heterogeneous private and public clouds and across all cloud layers (IaaS/PaaS/SaaS) (ETSI, 2013).

In a federated cloud scenario, a cloud provider sub-contracts capacity from other providers as well as offer spare capacity to a federation of cloud providers. Parts of a service are placed on remote providers for improved elasticity and fault tolerance, but the initial cloud provider is solely responsible for guaranteeing the agreed upon SLA. The federated cloud scenario is related to community cloud set-ups, or from a commercial perspective, for cloud providers that own multiple cloud islands in diverse regions, to balance workload among them.

In a multi-provider scenario, a broker acting on behalf of the user is responsible for the management of multi-cloud provisioning of the services. Access to this functionality can be provided either directly or through a cloud marketplace to hide management complexity. The user, or an acting-broker, contacts all possible cloud providers, negotiates terms of use, deploys services, monitors their operation, and potentially migrates services (or parts thereof) from misbehaving cloud providers. Cloud providers are managed independently and placement on different providers is treated as multiple instances of deployment.

There are several motivations for embracing brokering multi-cloud set-ups both from a provider and customer's perspectives.

Table 1:Providers and customers perspective for embracing multi-cloud brokering.

Provider perspective	Customer perspective
Scalability and wide resource availability	Avoid vendor lock-in
Cost efficiency and energy savings	Geographic distribution for low latency access, legal constraints and high availability

Cloud marketplaces are emerging to offer a mixture of service management, cloud deployment automation and application assembly, often in multi-cloud environments. Cloud providers such as Amazon WS (AWS Marketplace, n.d.), HP (HP, n.d.) or IBM (IBM, n.d.) have already launched their own cloud marketplace services, while other big players such as Cisco (CISCO dCloud, 2015) or Oracle (ORACLE, 2015) are launching their solutions for the public sector offering their products as a service. At the same time, both commercial solution providers (such as Appcara AppStack (Appcara, n.d.) and Jamcracker Service Delivery Network ((JSDN), n.d.)) and Open Source initiatives (Ubuntu Juju (Ubuntu, n.d.)) are developing solutions that enable the creation of customized cloud marketplaces. These integrate the APIs of several cloud platforms in order to automate the assembly of complex applications, its deployment and operation on one or multiple cloud infrastructure.

Table 2. Key features and related challenge

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

Targeting specifically the European research community, Helix Nebula Marketplace (Nebula, n.d.) has been established by a combination of public and private organizations, to provide data to intensive science with a multidisciplinary and multi-cloud platform. Helix Nebula service is offered by federation between European cloud vendors (Atos, CGI, CloudSIgma, EGI, Interoute, SixSq, The Server Labs and T-Systems) and science organizations (CGI, EGI and GÉANT) specifically addressing European legal and regulatory requirements.

At the same time, Government cloud marketplaces continue to growth in number and influence. Gov.apps (Gov.apps, n.d.) in the US was the first one to appear, but soon others have summed up to this trend: UK with Digital Marketplace (previously CloudStore (UK Government, n.d.) offered under G-Cloud) and other on-going initiatives in Australia (Australian Government, 2015) and New Zealand (New Zealand Department of Internal Affairs (DIA), n.d.). 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.

3.3 Current practices in Cloud Services Brokers

During the SOTA phase of the current research an analysis of the most relevant existing Cloud Broker Solutions has been performed. Different nature solutions have been evaluated: Commercial CB solutions/Open Source CB solutions/ EU funded projects results based solutions, Government Cloud Marketplaces. In the following pictures the coverage of the different solutions with respect to the key features described in table 2 is presented. (0- Not Known, 1-Not covered, 2-Partially covered, 3-Fully covered):

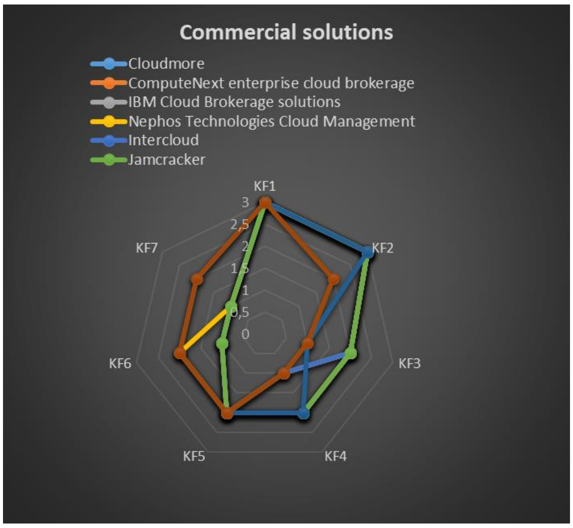

Figure 1:Analysed commercial solutions coverage of the key features

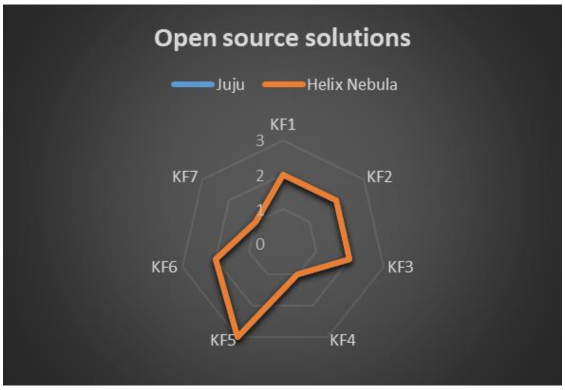

Figure 2: Analysed open source solutions coverage of the key features

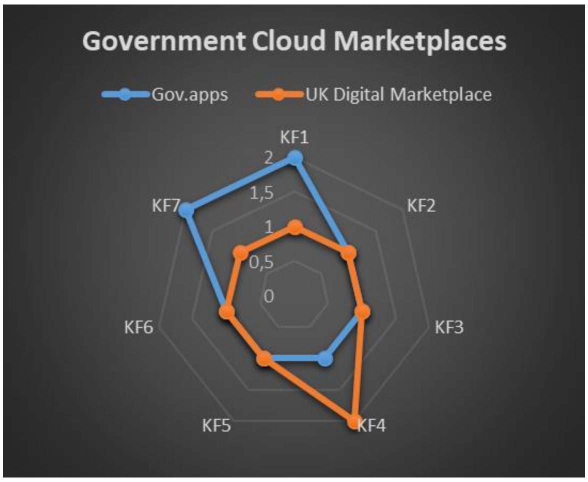

Figure 3:Government Cloud Marketplaces coverage of the key features

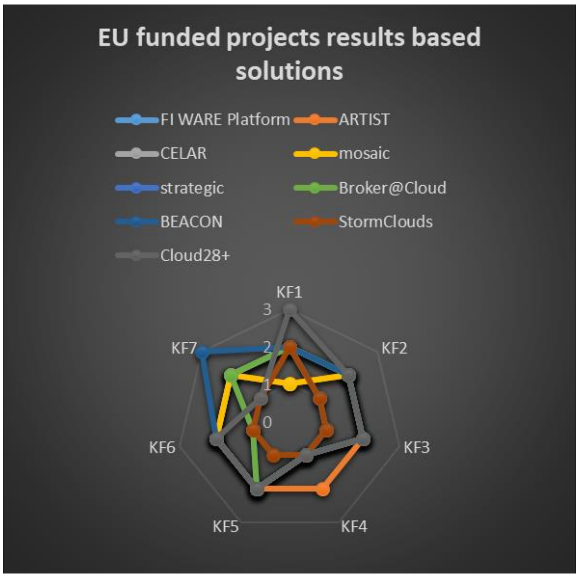

Figure 4: EU funded projects results based solutions coverage of the key features

From these graphics several conclusions can be extracted:

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

4 METHODOLOGY

To be able to execute research, there are many research methods and data collection techniques available to follow in order to achieve the research finding. However, the selection of research method depends on problem in hand.

The overall approach of the research cycle followed is shown in Figure 1.

First, we explored the current situation, practices and technology, and the need for overcoming the challenges of the current research problem, including current practice in Service Brokers, modelling dynamic and re-configurable multi-cloud applications, DevOps paradigms, relevant standards, certification schemes and legislations. These topics were examined and discussed together with its main aspects with relevant stakeholders (technology providers, software integrators, software consumers, research institutions). Based on this exploration, we could revisit and refine the research problem to identify more detailed assumptions, and we could formulate a theory for the needed design software development solution. This research was enriched with a cycle of “research in design context” for the specification of the requirements derived from the concrete use cases where the solution is to be applied. These activities have been focused in three potential use case contexts: eHealth, Network management and High Availability. Confirmative research actions were carried out to justify, validate and consolidate the research activities, methods and findings, through four phases.

Following this approach, the iterative and incremental (spiral) development approach has produced a 1st set of specifications and implementation to quickly proceed with the development and use case activities, then an intermediate version that takes into account some initial feedbacks and provides additional and more refined features, and a final version that takes into account use cases’ validation hints and feedbacks as well as implements new features addressing new possible requirements that emerged during the validations. This development strategy will ensure a smooth elaboration of results, with almost immediate feedback from the community and synchronization with user requirements and the latest technology trends.

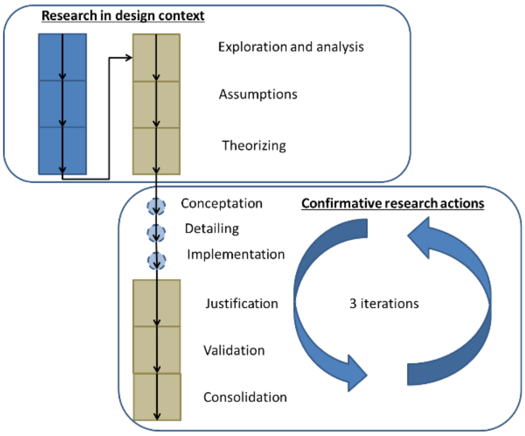

Figure 5:Proposed research methodology

The validation is expected to be performed in the following scenarios:

- Experiment 1: High availability – network management
- Experiment 2: eHealth – Clinical Research Platforms
- Experiment 3: Network Management in Telecoms Operators

These experiments have been selected considering real scenarios where the application of multi-cloud software is relevant. Different needs related to the non-functional requirements will be validated depending on the concrete necessities. i.e: scenario 1 will be focused n availability NFR while scenario 2 will be focused on legal awareness.

5 EXPECTED OUTCOMES

5.1 Research questions

This thesis proposes a major hypothesis:

H-It is possible to demonstrate that the proposed ACSmI can contribute to the creation of an ecosystem of trusted, interoperable and legal compliant cloud services fostering the uptake of cloud computing, with a special focus on multi-cloud aware applications that have specific non-functional requirements.

This hypothesis can be broken down into the following ones:

- H1- It is possible to define the multi-cloud concept and demonstrate its validity in real use case scenarios.Multi-cloud concept as referred to applications that can dynamically distribute their components (pieces of the application, snippets of code) over heterogeneous cloud resources and still hold the functional, business and non-functional properties (NFP) declared in their SLAs. The real use cases where to demonstrate the validity will be High availability – online gaming, eHealth – Clinical Research Platforms and Network management. These use cases have been selected bearing in mind the requirements and needs of those type of software applications that need to be legally aware and compliant, and need to fulfil high demanding requirements of performance, availability and reliability, without reaching high costs. Along with the multi-cloud concept, the Multi Cloud Service Level agreement (MCSLA) shall be defined.
- H2-It is possible to discover, benchmark and select the best combination of Cloud Services based a set of specific non-functional requirements elicited by the end-user. This hypothesis tries to prove the possibility of intelligent discovery of Cloud Services following a resource-centric approach, searching always for the best opportunistic choices while fulfilling the requirements set by the user. These requirements shall include non-functional properties, such as cost or availability and also total or partial compliance with respect to relevant legislation.
- H3-It is possible to assess and monitor the fulfilment of non-functional requirements against composed CSLAs and legislation and react to the violation of these requirements.In order to remain sustainable, a cloud based application cannot stop its operation and it is expected that it is self-adaptive with respect to the new topology needed to fulfil the users' requirements at all times. That is why the dynamic monitoring of NFRs as set by the user or potential SLA violations must be assessed and monitored. The composed CSLAs (the service level agreement that the application will offer to end-users (MCSLA)) be influenced by the SLAs of the underlying

(combination of) cloud services to be contracted.

- H4-It is possible to increase the automation of the portability of an application to a new Cloud service provider while ensuring the predefined set of non-functional requirements. Means to ensure the seamless change of Cloud Service Provider easing the data transfer mechanism between different cloud services shall be provided. The use and interoperability between services using non-standard and proprietary data formats and protocols to communicate through specific connectors will be improved providing the necessary means to execute the migration process necessary for data portability.
- H5-It is possible to demonstrate the dependency of the business model and the technical design in Cloud Broker solutions. Definition of “broker for benefit” concept, business model and related negotiated services, in order to support negotiated access and usage of the broker, exploring different business models and establishing the required modules to execute those business models, analysing the existing dependency between the business model an the architectural components of the Cloud Broker solution.

5.2 Thesis outputs and scientific contributions

Pursuing the above goals, we are expecting to achieve several scientific contributions. The main scientific results and contributions from this Thesis are the following:

- Result 1-Multicloud aware concept – Demonstrates H1
- Result 2-ACSmI-Demonstrates H2-H5

5.2.1 MultiCloud aware concept

The objective of this research is to analyse, describe and characterize multi-cloud native applications that will ease the design, development, optimization and deployment of multi-cloud native applications.

This characterization can be made through different type of architectural patterns (i.e. patterns for implementation, patterns for optimization and patterns for deployment), each covering different phases of the software development lifecycle (SDLC). These multi-cloud architectural patterns will allow the design and development of distributed applications over heterogeneous cloud resources whose components are prepared to be optimally deployed on different cloud service providers (CSPs) and still, they all work in an integrated way and transparently for the end-user.

5.2.2 ACSmI

Advanced Cloud Service meta-Intermediator is the platform that will demonstrate the major hypothesis of this thesis.

The Advanced Cloud Service (meta-) intermediator (ACSmI) (DECIDE Consortium, 2017) aims to provide the means for the discovery, contracting, managing and monitoring of different cloud service offerings. ACSmI will provide 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 as the different phases that a cloud service will pass through during their lifecycle in the ACSmI.

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

To be able to support these activities the proposed ACSmI technical architecture is shown in the following Figure 6.

There are four main components in charge of the implementation of the core functions explained above. Following, a high-level description of the main components and their corresponding sub-components is presented.

- Service Management. This component is in charge of 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 by this component and the corresponding sub-components.
- Cloud service SLA monitoring. This module is in charge of managing 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) assessment of the compliance of the SLA of the contracted services and 4) notification of the SLA violation to the CSP.

- Legislation Compliance. This component is responsible for 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 is in charge of the execution and management 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.

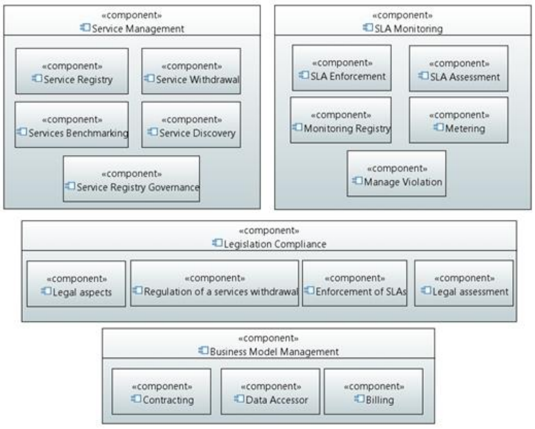

Figure 6: ACSmI High level architecture

6 STAGE OF THE RESEARCH

Currently the research is in the implementation stage (see Figure 5) under confirmative research actions phase. The state of the art, definition of the Hypothesis, requirements and technical design have been completed. The technical implementation has been started and the main functionalities completed and tested. The second iteration of the implementation is currently active addressing the feedback received from the first evaluation by the end users and continuing with advanced functionalities.

ACKNOWLEDGEMENTS

The project leading to this paper has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731533.

REFERENCES

Iyer, G. & Ganesh, N., 2012. *Broker-Mediated Multiple-Cloud Orchestration Mechanisms for Cloud Computing.*, s.l.: s.n.

(JSDN), J. S. D. N., n.d. *Jamcracker Services Delivery Network (JSDN).* [Online] Available at: http://www.jamcracker.com/jamcracker-services-delivery-network-jsdn
[Accessed 2019].

Alonso, J., 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.* Rome, s.n.

Alonso, J., Orue-Echevarria, L., Escalante, M. & Benguria, G., 2017. *Federated Cloud Service Broker (FCSB):an Advanced Cloud Service Intermediator for Public Administrations.* Oporto, s.n.

Appcara, n.d. *AppStack by.* [Online] Available at: http://www.appcara.com/products/appstack-r3
[Accessed 2019].

Australian Government, 2015. *Collaboration, Services and Skills.* [Online] Available at: http://www.finance.gov.au/collaboration-services-skills/
[Accessed 24th February 2016].

AWS Marketplace, n.d. *AWS Marketplace.* [Online] Available at: https://aws.amazon.com/marketplace
[Accessed 09 07 2019].

CISCO dCloud, 2015. *CISCO dCloud.* [Online] Available at: https://dcloud-lon-web-1.cisco.com/dCloud/
[Accessed 2019].

DECIDE Consortium, 2017. *D5.1 ACSmI requirements and technical design.* [Online]
[Accessed April 2018].

ETSI, 2013. *Cloud Standards Coordination - Final Report,* s.l.: s.n.

Gov.apps, n.d. *Gov.apps.* [Online] Available at: https://en.wikipedia.org/wiki/Apps.gov [Accessed 2019].

HP, n.d. *HP Helion.* [Online] Available at: https://marketplace.hpcloud.com/ [Accessed 21 May 2015].

IBM, n.d. *IBM Cloud.* [Online] Available at: http://www.ibm.com/cloud-computing/us/en/marketplace.html
[Accessed 21 May 2015].

Leire Orue-Echevarria Arrieta, J. A. I. J. G. H. R., 2011. *FROM SOFTWARE-AS-A-GOOD TO SAAS: CHALLENGES AND NEEDS: Developing a tool supported methodology for the migration of non-SaaS applications to SaaS.* s.l., s.n.

Mazzuca, J., 2015. *Survey Analysis: Cloud Adoption Across Vertical Industries Exhibits More Similarities Than Differences,* s.l.: Anderson.

Mell, P. & Grance, T., 2011. *The NIST definition of Cloud Computing,* Gaithersburg USA: Information Technology Laboratory. National Institute of Standards and Technology.

Nebula, H., n.d. *Helix Nebula Maarketplace.* [Online] Available at: http://hnx.helix-nebula.eu/ [Accessed 2019].

New Zealand Department of Internal Affairs (DIA), n.d. *DIA's Government Technology Services (GTS).* [Online]
Available at: http://www.standards.co.nz/news/media-releases/2009/dec/leveraging-government-shared-services-standards-new-zealand-works-with-government-technology-service/
[Accessed 2019].

Nizamani, S. A., 2012. *A Quality-aware Cloud Selection Service for Computational Modellers* , s.l.: s.n.

ORACLE, 2015. *Oracle iGovernment.* [Online] Available at: http://www.oracle.com/us/industries/public-sector/cloud-solutions-public-sector-wp-323002.pdf
[Accessed 2019].

Petcu, D., 2013. *Multi-Cloud: Expectations and Current Approaches..* New York, s.n.

Ubuntu, n.d. *Ubuntu Juju,.* [Online] Available at: http://community.ubuntu.com/ [Accessed 21 05 2015].

UK Government, n.d. *Gov UK Digital Marketplace.* [Online]
Available at: https://www.digitalmarketplace.service.gov.uk/
[Accessed 2019].

US Government Accountability Office, 2012. *Progress Made but Future Cloud Computing Efforts Should be Better Planned,* http://www.gao.gov/assets/600/592249.pdf.: Retrieved February 2015.

Vliet, J. v. & Paganelli, F., 2011. *Programming Amazon EC2.* 1st ed. s.l.:O'reily media.